FEB 27 2009
PATENT & TRADEMARK OFFICE

AF/IDW

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE HONORABLE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of

Kazuma AOKI et al.

On Appeal from Group: 2454

Application No.: 10/671,686

Examiner: M. KEEFER

Filed: September 29, 2003

Docket No.: 117025

For: COMMUNICATION DEVICE PREVENTING UNAUTHORIZED ACCESS TO ITS SERVICES VIA USER INTERVENTION AND A METHOD THEREOF

APPEAL BRIEF TRANSMITTAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is the Brief on Appeal in the above-identified application.

Also attached is Check No. 215695, in the amount of $540.00 ($270.00 Small Entity), in payment of the fee due under 37 C.F.R. 41.20(b)(2).

In the event of any underpayment or overpayment, please debit or credit Deposit Account No. 15-0461 as needed in order to effect proper filing of this Brief.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Scott M. Schulte
Registration No. 44,325

JAO:SMS/bab

Date: February 27, 2009

OLIFF & BERRIDGE, PLC
P.O. Box 320850
Alexandria, Virginia 22320-4850
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

FEB 27 2009
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE HONORABLE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of

Kazuma AOKI et al.

Application No.: 10/671,686 Examiner: M. KEEFER

Filed: September 29, 2003 Docket No.: 117025

For: COMMUNICATION DEVICE PREVENTING UNAUTHORIZED ACCESS TO ITS SERVICES VIA USER INTERVENTION AND A METHOD THEREOF

BRIEF ON APPEAL

Appeal from Group 2454

OLIFF & BERRIDGE, PLC
P.O. Box 320850
Alexandria, Virginia 22320-4850
Telephone: (703) 836-6400
Fax: (703) 836-2787
Email: email@oliff.com
Attorneys for Appellants

03/02/2009 JADD01 00000064 10671686
01 FC:1402 540.00 OP

I. REAL PARTY IN INTEREST

The real party in interest for this appeal and the present application is Brother Kogyo Kabushiki Kaisha, by way of an Assignment recorded in the U.S. Patent and Trademark Office at Reel 014555, Frame 0572.

II. STATEMENT OF RELATED CASES

There are no prior or pending appeals, interferences or judicial proceedings, known to any inventor, any attorney or agent who prepared or prosecuted this application, or any other person who was substantively involved in the preparation or prosecution of this application, that may be related to, or that will directly affect or be directly affected by or have a bearing upon, the Board's decision in the pending appeal.

III. JURISDICTIONAL STATEMENT

The Board has jurisdiction under 35 U.S.C. §134(a). The Examiner mailed a Final Rejection on September 3, 2008, setting a three-month shortened statutory period for response. The time for responding to the Final Rejection expired on December 3, 2008. Rule 134. A Notice of Appeal and a Petition for Extension of Time requesting a one-month extension of time under Rule 136(a) were filed on January 5, 2009. The time for filing an Appeal Brief expires the later of two months from the filing of the Notice of Appeal, or one month from the mailing date of the Notice of Panel Decision if a Pre-Appeal Brief Request for Review is sought. Bd.R. 41.37(c) and Official Gazette Notice, July 12, 2005.

No Pre-Appeal Request for Review was sought. The extendible period for filing the Appeal Brief therefore expires March 5, 2009. This appeal brief is being timely filed on February 27, 2009.

IV. TABLE OF CONTENTS

Page

I. Real Party In Interest 2

II. Statement Of Related Cases 3

III. Jurisdictional Statement 4

IV. Table Of Contents 5

V. Table Of Authorities 7

VI. Status Of Amendments 8

VII. Grounds Of Rejection to Be Reviewed 8

VIII. Statement Of Facts 10

A. Technical Background And Prior Art 10

B. WAN/LAN Request Determining Feature Of Independent Claims 1 And 11 12

C. Automatic Acceptance Of LAN Request Feature Of Independent Claims 1, 11 And 20 15

D. User Acceptance Of WAN Request Feature Of Independent Claims 1, 11 And 20 19

E. User Acceptance Of Online Real-Time Processing Request Feature Of Dependent Claims 7 And 16 22

F. Other Dependent Claims 24

IX. Argument 25

A. Susaki And Shitama Fail To Disclose Or Suggest The Processing Of Requests That Come In From The LAN And/Or The WAN As Defined In Independent Claims 1, 11 And 20 25

1. Susaki And Shitama Both Fail To Discuss Determining Whether Requests Come In From The WAN Or The LAN As Required By Independent Claims 1 And 11 26

2. Susaki And Shitama Fail To Suggest The Handling Of Requests That Come In From The LAN As Defined In Independent Claims 1, 11 And 20 28

3. Susaki And Shitama Fail To Suggest The Handling Of Requests That Come In From The WAN As Defined In Independent Claims 1, 11 And 20 33

4. Summary 36

B. Susaki And Shitama Fail To Suggest Demanding A Determination Only For Requests That Involve Real-Time Processing As Required By Dependent Claims 7 And 16 37

C. Dependent Claims 37

X. Conclusion 38

XI. APPENDIX A - Claims Section 39

XII. APPENDIX B - Claim Support and Drawing Analysis Section 45

XIII. APPENDIX C - Means or Step Plus Function Analysis Section 49

XIV. APPENDIX D - Evidence Section 50

XV. APPENDIX E - Related Cases Appendix 219

V. TABLE OF AUTHORITIES

Cases — Page

KSR v. Teleflex, 550 U.S. 398 (2007) 28, 32, 36

Statutes

35 U.S.C. §103(a) 28, 32, 36

Other Authorities

Examination Guidelines for Determining Obviousness under 35 U.S.C. §103 in View of the Supreme Court Decision in *KSR International Co. v. Teleflex Inc.* 28, 32, 36

VI. STATUS OF AMENDMENTS

No Amendment After Final Rejection has been filed. Appellants instead filed a Request for Reconsideration on December 2, 2008, which was considered as evidenced by the December 23, 2008 Advisory Action.

VII. GROUNDS OF REJECTION TO BE REVIEWED

The following grounds of rejection are presented for review:

1) Claims 1, 3, 6, 7, 9, 11, 13, 15-18 and 20[1] are rejected as having been obvious under 35 U.S.C. §103(a) over Susaki et al. (Susaki), U.S. Patent No. 6,189,032, in view of Shitama, U.S. Patent Application Publication No 2002/0110123.

2) Claims 2 and 12 are rejected as having been obvious under 35 U.S.C. §103(a) over Susaki in view of Shitama and Joubert et al. (Joubert), U.S. Patent No. 6,101,616.

3) Claims 5 and 14 are rejected as having been obvious under 35 U.S.C. §103(a) over Susaki in view of Shitama and Allen et al. (Allen), U.S. Patent Application Publication No. 2003/0041333.

---

[1] The Office Action does not formally reject claims 4 and 8; however, pages 3 and 4 of the Office Action discuss the claims in view of Susaki. To the extent that claims 4 and 8 stand rejected, they are included herewith.

4) Claims 10 and 19 are rejected as having been obvious under 35 U.S.C. §103(a) over Susaki in view of Shitama and Boehmke et al. (Boehmke), U.S. Patent Application Publication No. 2002/0126822.

VIII. STATEMENT OF FACTS

A. Technical Background And Prior Art

1. Appellants' invention is directed to a communication device and a method of communicating with a communication device that is connected to a LAN (local area network) and a WAN (wide area network), and can perform a predetermined process (for example, printing, faxing, or changing the settings of the communication device by remote control) according to requests made by LAN terminals and/or WAN terminals (paragraphs [0001], [0045], [0060] and [0061] of Appellants' specification).

2. Appellants' communication device includes a first input portion connected with a wide area network (WAN) (WAN port 6, Appellants' Fig. 2, claims 1, 11 and 20); and a second input portion connected with a local area network (LAN) (LAN port 7, Appellants' Fig. 2, claims 1, 11 and 20).

3. Appellants' controller or method will either automatically accept an operation according to the request every time that it is determined that the request came in from the LAN (Appellants' step S2, Fig. 3, paragraph [0038], claims 1 and 11), or allow a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the

WAN (Appellants' step S2: YES, step S5, Fig. 2; steps S21-S24, Fig. 4, Fig. 6, paragraphs [0041] - [0043] and [0051], claims 1 and 11).

4. Thereafter, predetermined processing is allowed to be performed according to the request when a performance of the operation according to the request is accepted - either automatically or via a user (Appellants' step S2: NO, step S7: YES, step S8, Fig. 3, claims 1 and 11).

5. Appellants are thus able to overcome the problems associated with passwords being leaked to unauthorized users or having unauthorized users use the communication device (Appellants' paragraph [0003]).

6. Susaki is directed to a client-server system in which access to a service by a user can be properly controlled, even if approval by another user is sometimes required for receiving the service (Susaki's Abstract).

7. In particular, Susaki uses a process control rule to determine whether requests are automatically accepted or whether user approval is necessary (Susaki's col. 9, lines 29 - col. 10, line 17).

8. Susaki is directed to terminals that are connected to a LAN (Susaki's col. 1, lines 16-21 and col. 6, lines 8-12).

9. Susaki is thus able to control access to a particular service by a user connected to a LAN in order to avoid leaking official secrets and the falsification of information (Susaki's col. 1, lines 31-37).

10. Susaki does not disclose that all requests are automatically accepted or that all requests require user approval.

11. Susaki also does not disclose a WAN or otherwise refer to a WAN.

12. Shitama is directed to a network connection control apparatus and method that grants access by an authenticated device on a global network to a device on a local network (Shitama's Abstract).

13. In particular, Shitama uses an authentication unit 302 that automatically authenticates a device on a WAN according to a predetermined authentication method and procedure (Shitama's paragraph [0043]).

14. Shitama does not disclose allowing a user to approve any requests.

15. Shitama also does not disclose how requests from a LAN are processed or whether or not security is applied to requests from a LAN.

B. WAN/LAN Request Determining Feature Of Independent Claims 1 And 11

16. Independent claim 1 recites, *inter alia*, a controller that determines whether a request to perform predetermined processing came in from the WAN or the LAN.

17. Independent claim 11 recites, *inter alia*, a step of determining whether a request to perform predetermined processing came in from the WAN or the LAN.

18. The Examiner rejected claims 1 and 11 for obviousness over Susaki in view of Shitama, asserting, *inter alia*, that the references suggest the features of claims 1 and 11 identified in facts 16 and 17 (Office Action, pages 2, 5 and 6).

19. More particularly, page 2 of the Office Action states that Susaki (col. 9, lines 38-48) discloses a controller that determines whether a request to perform predetermined processing came in from the WAN or the LAN.

20. Appellants respectfully disagree with the Office Action assertions in facts 18 and 19.

21. Susaki's Fig. 1 and col. 6, lines 8-12 disclose terminals 1 and a server 2 mutually connected through a communication network 3 such as a LAN.

22. Susaki's col. 9, lines 38-48 disclose using the server 2 to retrieve a user authority level and a process control rule specified in correspondence with the user authority level for a terminal 1 connected via the LAN.

23. Susaki does not disclose that the process of the controller determining whether a request requires the approval of another user, as asserted on page 2 of the Office Action, is based on, or otherwise involves, a determination about whether a request comes in from the LAN or the WAN.

24. Susaki does not use the term "WAN" or otherwise refer to a "WAN."

25. Thus, Susaki does not disclose a controller that determines, or the step of determining, whether a request to perform predetermined processing came in from the WAN or the LAN as recited in claims 1 and 11.

26. The Advisory Action, on lines 4-5 of the continuation sheet, states that "the Examiner points to paragraphs 52-53 [of Shitama], which disclose determining that a request came from a WAN (as opposed to the LAN)

by determining what interface the request arrived from (Fig. 2, interfaces 33 and 34)."

27. Appellants respectfully disagree with the Advisory Action assertion in fact 26.

28. Shitama's paragraph [0052] states that the service access request message is received via the WAN-side interface unit 33 in step S1.

29. Shitama's paragraph [0053] states that the source IP address and the source port number contained in the IP header of the received service access request message, indicating the transmitting device, are confirmed, and the device which transmitted the service access request message is authenticated.

30. Shitama's paragraphs [0052] and [0053], asserted in the Advisory Action, do not disclose that a determination is made as to whether a request to perform predetermined processing came in from the WAN or the LAN, or indicate that such a determination is necessary or desirable.

31. Shitama's paragraph [0043] discloses an authentication unit 302 that, upon receiving a packet from the WAN-side interface 33, automatically authenticates a device connected to the WAN according to a predetermined authentication method and procedure.

32. Shitama's paragraph [0043] does not disclose that it is necessary or desirable for the authentication unit 302 to determine if a request came from a WAN (as opposed to the LAN).

33. Thus, Shitama does not disclose a controller that determines, or the step of determining, whether a request to perform predetermined processing came in from the WAN or the LAN as recited in claims 1 and 11.

34. In conclusion, Susaki and Shitama, neither alone nor in combination, disclose(s) the features of claims 1 and 11 set forth in facts 16 and 17.

C. Automatic Acceptance Of LAN Request Feature Of Independent Claims 1, 11 And 20

35. Independent claim 1 recites, *inter alia*, a controller that automatically accepts an operation according to the request every time that it is determined that the request came in from the LAN.

36. Independent claim 11 recites, *inter alia*, a step of automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN.

37. Independent claim 20 recites, *inter alia*, a controller that automatically performs predetermined processing according to a request every time that a performance of an operation is requested by a LAN.

38. The Examiner rejected claims 1, 11 and 20 for obviousness over Susaki in view of Shitama, asserting, *inter alia*, that the references suggest the features of claims 1, 11 and 20 identified in facts 35-37 (Office Action, pages 5 and 8-10).

39. More particularly, page 5 of the Office Action states that the concept of automatically allowing all requests from the LAN are well known in the art as taught by Shitama.

40. The Advisory Action, on lines 9-11 of the continuation sheet, further states that "since no scrutiny is applied to requests from the LAN in SHITAMA, one of ordinary skill in the art would be motivated to continue to trust all requests from the LAN."

41. Appellants respectfully disagree with the Office Action and Advisory Action assertions in facts 38-40.

42. Shitama's paragraph [0029] states that the terminal device 50 is connected to the local network 20.

43. Shitama does not disclose how the terminal device 50 communicates with other devices on the LAN.

44. Shitama does not disclose how requests from the LAN are treated or otherwise indicate whether security is or is not applied to requests from the LAN.

45. Shitama is instead directed to granting access by an authenticated device on the WAN to a device on the LAN (Shitama's Abstract)

46. Shitama thus does not disclose the concept of automatically allowing all requests from the LAN.

47. Shitama thus does not disclose that no scrutiny is applied to requests from the LAN.

48. Therefore, Shitama does not disclose automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN as recited in claims 1 and 11, or automatically performing predetermined processing according to a request every time that a performance of an operation is requested by a LAN as recited in claim 20.

49. Susaki discloses security for requests that originate from the LAN (Susaki's col. 1, lines 16-21 and col. 6, lines 8-12).

50. Page 12 of the Office Action states that it does not hold that all of the levels of scrutiny in Susaki must be used in combination with Shitama.

51. Page 13 of the Office Action also states that, in combination with Susaki, one of ordinary skill in the art at the time of the invention would place all LAN addresses as having a user authority level of "0" (i.e., always processable).

52. Appellants respectfully disagree with the Office Action assertions in facts 50 and 51.

53. Susaki's col. 9, lines 58-67 state that, if the process control rule indicates that an approval is not required, the service approval request processor 206 does not transmit an approval request.

54. Susaki's col. 10, lines 1-17 state that, if the process control rule indicates that approval by a user is required, the service approval request processor 206 transmits an approval request.

55. In other words, Susaki's col. 10, lines 1-17 disclose that a user must authenticate some requests that originate from the LAN, and thus Susaki does not automatically accept all requests from the LAN.

56. Susaki does not disclose that all levels of scrutiny are not used.

57. Susaki also does not disclose that all LAN addresses would have a user authority level of "0" as illustrated in Susaki's Fig. 5.

58. Susaki's col. 1, lines 31-37 instead disclose that it is necessary to control access to a particular service by a user in order to avoid leaking official secrets and the falsification of information.

59. Therefore, Susaki does not disclose automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN as recited in claims 1 and 11, or automatically performing predetermined processing according to a request every time that a performance of an operation is requested by a LAN as recited in claim 20.

60. Shitama's paragraph [0006] also discloses the need to prevent resources in the terminal devices, such as the individual servers on the local network, from being destroyed or having their secret contents leaked by external illegal access.

61. In conclusion, Susaki and Shitama, neither alone nor in combination, disclose(s) the features of claims 1, 11 and 20 as set forth in facts 35-37.

D. User Acceptance Of WAN Request Feature Of Independent Claims 1, 11 And 20

62. Independent claim 1 recites, *inter alia*, a controller that allows a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN.

63. Independent claim 11 recites, *inter alia*, a step of allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN.

64. Independent claim 20 recites, *inter alia*, a controller that allows a user of the communication device to determine whether an operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN.

65. The Examiner rejected claims 1, 11 and 20 for obviousness over Susaki in view of Shitama, asserting, *inter alia*, that the references suggest the feature of claims 1, 11 and 20 identified in facts 62-64 (Office Action, pages 2, 6 and 9).

66. More particularly, page 2 of the Office Action states that Susaki discloses a controller that allows a user of the communication device to determine whether an operation according to the request is accepted or rejected when it is determined that the request came in from the WAN.

67. The Examiner argues (Office Action, page 2) that Susaki's col. 10, lines 1-7 disclose the features of claims 1, 11 and 20 set forth in facts 62-64 because Susaki describes how a user is allowed to determine whether a request is allowed or rejected.

68. Appellants respectfully disagree with the Office Action assertions in facts 65-67, particularly given that the Office Action fails to assert that Susaki discloses the "every time" feature of claims 1, 11 and 20 set forth in facts 62-64.

69. As discussed above, Susaki does not disclose a "WAN" or otherwise refer to a "WAN."

70. Susaki's col. 10, lines 1-17 disclose that, if the process control rule indicates that approval by a user is required, the service approval request processor 206 transmits an approval request.

71. However, Susaki's col. 9, lines 58-67 also disclose that, if the process control rule indicates that an approval is not required, the service approval request processor 206 does not transmit an approval request.

72. In other words, Susaki col. 9, lines 58-67 disclose that some requests that originate from the LAN are automatically accepted, and thus a user does not authenticate all requests from the LAN.

73. Therefore, Susaki does not disclose allowing a user of the communication device to determine whether the operation according to

the request is accepted or rejected every time that it is determined that the request came in from the WAN as recited in claims 1, 11 and 20.

74. The Advisory Action, on lines 5-7 of the continuation sheet, states that one of ordinary skill in the art would have been motivated to replace the security system provided by Shitama in gateway 30 with the security system provided by Susaki in order to allow access to a service to be properly controlled.

75. Appellants respectfully disagree with the Advisory Action assertion in fact 74.

76. Shitama's paragraph [0043] discloses an authentication unit 302 that, upon receiving a packet from the WAN-side interface 33, automatically authenticates a device connected to the WAN according to a predetermined authentication method and procedure.

77. Shitama does not disclose allowing a user to authenticate any request from the WAN.

78. As discussed above, Susaki col. 9, lines 58-67 disclose that some requests that originate from the LAN are automatically accepted, and thus a user does not authenticate all requests from the LAN.

79. Thus, if the security system provided by Susaki replaced the security system provided by Shitama in gateway 30 as asserted in the Advisory Action in fact 74 (a substitution that Appellants do not admit would have

been obvious), some requests from the WAN would still be automatically accepted.

80. Therefore, when combined, Susaki and Shitama fail to disclose allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN as recited in claims 1, 11 and 20.

81. In conclusion, Susaki and Shitama, neither alone nor in combination, disclose(s) the features of claims 1, 11 and 20 as set forth in facts 62-64.

E. User Acceptance Of Online Real-Time Processing Request Feature Of Dependent Claims 7 And 16

82. Claim 7 depends from claim 1 and further recites a controller that demands the user of the communication device to determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing, which is a specified request from the WAN.

83. Claim 16 depends from claim 11 and further recites that the user of the communication device must determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing, which is a specified request from the WAN.

84. The Examiner rejected claims 7 and 16 for obviousness over Susaki in view of Shitama, asserting, *inter alia*, that the references suggest the features of claims 7 and 16 identified in facts 82 and 83 (Office Action, pages 3, 4 and 7).

85. More particularly, page 4 of the Office Action states that Susaki's col. 9, lines 42-48 disclose that not only is a user's authority taken into account when determining if a demand for approval is made to a user, but also the type of the request is taken into account.

86. Appellants respectfully disagree with the Office Action assertions in facts 84 and 85.

87. As discussed above, Susaki's col. 9, lines 38-48 disclose using the server 2 to retrieve a user authority level and a process control rule specified in correspondence with the user authority level for a terminal 1 connected via the LAN.

88. Susaki does not disclose requests that involve predetermined online real-time processing.

89. Susaki does not disclose that a user is demanded to or must determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing.

90. Shitama does not discuss predetermined online real-time processing.

91. In conclusion, Susaki and Shitama, neither alone nor in combination, disclose(s) the features of claims 7 and 16 as set forth in facts 82-83.

F. Other Dependent Claims

92. Claims 2-10 and 12-19 depend, directly or indirectly, from independent claim 1 or independent claim 11.

IX. ARGUMENT

A. Susaki And Shitama Fail To Disclose Or Suggest The Processing Of Requests That Come In From The LAN And/Or The WAN As Defined In Independent Claims 1, 11 And 20

Independent claim 1 recites a controller that (1) determines whether a request to perform predetermined processing came in from the WAN or the LAN; (2) automatically accepts an operation according to the request every time that it is determined that the request came in from the LAN; and (3) allows a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN. Independent claim 11 recites the steps of (1) determining whether a request to perform predetermined processing came in from the WAN or the LAN; (2) automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN; and (3) allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN. Independent claim 20 recites a controller that (2) automatically performs predetermined processing according to a request every time that a performance of an operation is requested by a LAN; and (3) allows a user of the communication device to determine whether an operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN.

The Examiner asserts that the combination of Susaki and Shitama discloses all of the features (1) - (3) numbered above of claims 1, 11 and 20 (pages 2-10 of the September 3, 2008 Final Office Action (hereinafter "Office Action"). In response, Appellants previously pointed out to the Examiner, as reargued below, why the Examiner is believed to have erred regarding each of the features (1) - (3) of claims 1, 11 and 20 (pages 2-5 of the November 2, 2008 Request for Reconsideration (hereinafter "Request"). The December 23, 2008 Advisory Action responds by repeating most of the arguments from the Office Action. Appellants herein traverse the rejection regarding each of the above-numbered features (1) - (3) of claims 1, 11 and 20.

1. Susaki And Shitama Both Fail To Discuss Determining Whether Requests Come In From The WAN Or The LAN As Required By Independent Claims 1 And 11

Claim 1 recites a controller that determines whether a request to perform predetermined processing came in from the WAN or the LAN (Fact 16); and claim 11 recites a step of determining whether a request to perform predetermined processing came in from the WAN or the LAN (Fact 17).

Susaki fails to disclose or suggest these features because Susaki fails to discuss the WAN or otherwise refer to the WAN (Fact 24). Susaki discloses a client-server system where terminals 1 and a server 2 are connected through a communication network 3 such as a LAN (Fig. 1 and col. 6, lines 8-12; Fact 21).

Page 2 of the Office Action states that Susaki discloses, at col. 9, lines 38-48, a controller that determines whether a request to perform a predetermined process came in from the WAN or the LAN (Fact 19). This is not correct (Fact 20) because Susaki does not even consider the WAN (Fact 24). In particular, col. 9, lines 38-48, cited on page 2 of the Office Action (Fact 19), fail to even mention the WAN (Facts 22-24).

The Advisory Action changes the position asserted in the Office Action by arguing that Shitama's paragraphs [0052] and [0053] allegedly disclose determining that a request came from the WAN (as opposed to the LAN) (Fact 26). Appellants disagree (Fact 27) because Shitama does not state or otherwise suggest that such a determination is needed or desired (Facts 30 and 32).

Shitama's paragraph [0052] states that the service access request message is received via the WAN-side interface unit in step S1 (Fact 28). Shitama's paragraph [0053] then states that the source IP address and the source port number contained in the IP header are confirmed, and the device that transmitted the service access request message is authenticated (Fact 29). Shitama's paragraph [0043] further explains that the authentication unit 302 automatically authenticates a device connected to the WAN according to a predetermined authentication method and procedure (Fact 31). Shitama does not state that a determination between the WAN or the LAN is made or otherwise refer to making such a determination (Facts 30 and 32).

The Examiner thus fails to provide a reasonable explanation as to why it would have been necessary or desirable for Shitama to determine whether a request came in from the WAN or the LAN, or explain how Shitama would have used such information.

A claimed feature is thus missing even after the references are combined, and such feature would not otherwise have been known or obvious so as to support a 35 U.S.C. §103(a) rejection in accordance with *KSR v. Teleflex*, 550 U.S. 398 (2007), and the U.S. Patent and Trademark Office Examination Guidelines for Determining Obviousness under 35 U.S.C. §103 in view of *KSR*.

Therefore, even if Susaki and Shitama were combined as suggested in the Office Action (which Appellants do not admit would have been obvious), the combination of Susaki and Shitama would not determine whether a request to perform predetermined processing came in from the WAN or the LAN as required by claims 1 and 11 (Facts 16 and 17).

2. Susaki And Shitama Fail To Suggest The Handling Of Requests That Come In From The LAN As Defined In Independent Claims 1, 11 And 20

Claim 1 recites a controller that automatically accepts an operation according to the request every time that it is determined that the request came in from the LAN (Fact 35); claim 11 recites a step of automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN (Fact 36); and claim 20 recites a controller that

automatically performs predetermined processing according to a request every time that a performance of an operation is requested by a LAN (Fact 37).

Shitama fails to disclose or suggest the above features because Shitama fails to discuss how requests are processed if they come in from the LAN (Fact 44). Rather, Shitama is directed to authenticating requests that come in from the WAN (Fact 45).

Shitama's paragraph [0029] simply states that a terminal device 50 is connected to the local network 20 (Fact 42). Shitama fails to disclose how the terminal device 50 communicates with other devices on the LAN (Fact 43). Shitama also fails to disclose how requests from the LAN are treated or otherwise indicate whether or not security is applied to requests from the LAN (Fact 44). Shitama further does not disclose the concept of automatically allowing all requests from the LAN or state that no scrutiny is applied to requests from the LAN (Facts 46 and 47).

Susaki fails to overcome the deficiencies of Shitama because a user authenticates some of the requests in Susaki that come in from the LAN (Facts 53-55). Susaki wants to control access to a particular service by a user connected via the LAN in order to avoid leaking official secrets and the falsification of information (col. 1, lines 31-37; Fact 58). In order to achieve this, Susaki, at col. 9, line 38 - col. 10, line 16, discusses using a service approval request processor 206 that determines if approval is required based on a process control rule (Facts 53 and 54). Based on the process control rule, a

determination is made whether approval is not required (col. 9, lines 58-67; Fact 53), or if approval is required (col. 10, lines 1-16; Fact 54). Because user approval may be required, Susaki does not automatically accept an operation according to a request every time that a request comes in from the LAN as required by independent claims 1, 11 and 20 (Facts 55 and 59).

Page 5 of the Office Action asserts that automatically allowing all requests from the LAN is a well-known concept (Fact 39). The Advisory Action also asserts that no scrutiny is applied to requests from the LAN in Shitama, and that one of ordinary skill in the art would have been motivated to continue to trust all requests from the LAN (Fact 40). Appellants disagree with these statements for at least four reasons (Fact 41).

First, Susaki (which explicitly discusses requests from the LAN (Fact 49)) does not automatically allow all requests from the LAN, and does not trust all requests from the LAN, because Susaki explicitly wants to control access to a particular service by a user connected via the LAN by creating a process control rule in order to avoid leaking official secrets and the falsification of information (Facts 55 and 58). Second, Shitama does not state that no scrutiny is applied to requests from the LAN, but rather is silent as to how requests from the LAN are treated (Fact 44). Third, Shitama's paragraph [0006] discusses the concern about having secret contents leaked by illegal access (Fact 60), thus suggesting that Shitama would actually want to add the security provided by Susaki's LAN to Shitama's LAN in order to prevent all

users connected via the LAN from having access to official secrets and to prevent the falsification of information. Fourth, as argued during the August 14, 2007 personal interview with Examiners Flynn and Keefer, Appellants assert that it is a well-known concept not to automatically allow all requests from the LAN, and that all requests from the LAN are not trusted. For example, a young attorney at a law firm does not have access to the same resources on the LAN as a senior partner, and a junior Examiner does not have access to the same resources on the LAN as the Commissioner for Patents.

Furthermore, page 12 of the Office Action asserts that it does not hold that all of the levels of scrutiny in Susaki must be used in a combination with Shitama (Fact 50). Page 13 of the Office Action also states that the combination of Shitama and Susaki suggests that all LAN addresses would have a user authority level of "0" as disclosed in Susaki's Fig. 5 (Fact 51).

Appellants disagree (Fact 52) because neither Susaki nor Shitama states that only user authority level "0" is used (Fact 57), and it is arbitrary to state that only user authority level "0" would have been used for requests that come in from the LAN. Appellants also assert that this is contrary to Susaki because Susaki has other process control rules that require user intervention (Fact 54). If Susaki was modified such that all LAN addresses would have a user authority level of "0", then Susaki would be rendered unsatisfactory for its intended purpose. Susaki seeks to control access to a particular service by a user connected via the LAN in order to avoid leaking official secrets and the

falsification of information (col. 1, lines 31-37; Fact 58). Shitama fails to overcome the deficiencies of Susaki given that Shitama does not focus upon the LAN (Facts 43-47). It is not reasonably predictable to discard the security provided for requests that come in from the LAN as discussed in detail by Susaki and to only apply scrutiny to requests that come in from the WAN in the manner suggested on pages 12 and 13 of the Office Action.

Appellants assert that, given the detail provided by Susaki as to how requests from the LAN are processed (Fact 49) and the lack of detail provided by Shitama (Facts 43-47), one skilled in the art combining the disclosures of Susaki and Shitama would logically have treated requests from the LAN as disclosed by Susaki (that is, some requests that come in from the LAN would require user approval (Fact 55)). If one skilled in the art were to have combined Susaki and Shitama (which Appellants do not admit would have been obvious), one skilled in the art would have added the LAN security disclosed by Susaki to the WAN security disclosed by Shitama.

A claimed feature is thus missing even after the references are combined, and such feature would not otherwise have been known or obvious so as to support a 35 U.S.C. §103(a) rejection in accordance with *KSR* and the U.S. Patent and Trademark Office Examination Guidelines for Determining Obviousness under 35 U.S.C. §103 in view of *KSR*. Therefore, even if Susaki and Shitama were combined as suggested in the Office Action (which Appellants do not admit would have been obvious), the combination of Susaki

and Shitama would not automatically accept an operation according to the request every time that it is determined that the request came in from the LAN as recited in claims 1 and 11, or automatically perform predetermined processing according to a request every time that a performance of an operation is requested by a LAN as recited in claim 20.

3. Susaki And Shitama Fail To Suggest The Handling Of Requests That Come In From The WAN As Defined In Independent Claims 1, 11 And 20

Claims 1 and 20 recite a controller that allows a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN (Facts 62 and 64); and claim 11 recites a step of allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN (Fact 63).

Page 2 of the Office Action asserts that Susaki discloses a controller that allows the user to determine whether a request is accepted or rejected from a WAN (Facts 66 and 67). Appellant notes in this regard that the Office Action fails to address the "every time" feature of claims 1, 11 and 20 (Fact 68). In any event, Appellants disagree with the Examiner's analysis because, as discussed above, Susaki fails to use the term "WAN" or otherwise refer to a "WAN" (Fact 69).

Appellant also disagrees with the Examiner's analysis because it does not consider all of Susaki's disclosure (Facts 70-72). Susaki's col. 10, lines 1-17 do disclose that, if the process control rule indicates that an approval by a user is not required, the service approval request processor 206 does not transmit an approval request (Fact 70). However, Susaki's col. 9, lines 58-67 also disclose that, if the process control rule indicates that an approval by a user is not required, the service approval request processor 206 does not transmit an approval request (Fact 71). Susaki thus discloses that some requests that originate from the LAN are automatically accepted, and thus a user does not authenticate all requests from the LAN (Fact 72).

The Advisory Action, on lines 5-7 of the continuation sheet, states that one of ordinary skill in the art would have been motivated to replace the security system provided by Shitama in gateway 30 with the security system provided by Susaki in order to allow access to a service to be properly controlled (Fact 74). Appellants disagree with this suggestion (Fact 75).

Shitama limits access from the WAN to the LAN by using an authentication unit 302 that, upon receiving a packet from the WAN-side interface 33, automatically authenticates a device connected to the WAN according to a predetermined authentication method and procedure (paragraph [0043]; Fact 76). Shitama does not disclose allowing a user to authenticate any request from the WAN (Fact 77). In fact, Shitama is precisely the type of art that suffers the same problems identified in paragraph [0003] of Appellants'

specification in that passwords may be artificially leaked to outsiders as well as being leaked by unauthorized users stealing packets from a network (Fact 5).

In addition, even if the security system provided by Susaki replaced the security system provided by Shitama in gateway 30 (which Appellants do not admit would have been obvious), the combination of Susaki and Shitama still fails to disclose all of the features of claims 1, 11 and 20 because some of the requests from the WAN would be automatically accepted (Fact 79). As discussed above, Susaki discloses that some of the requests that originate from the LAN are automatically accepted, and thus a user does not authenticate all requests from the LAN (Fact 78).

For similar reasons discussed above, Appellants assert that, given the detail provided by Shitama as to how requests from the WAN are processed (Fact 76) and the lack of any WAN detail by Susaki (Fact 69), if one skilled in the art were to have combined Susaki with Shitama (which Appellants do not admit would have been obvious), then one skilled in the art would have used Shitama's authentication procedure for requests that come in from the WAN. It would not have been reasonably predictable to discard Shitama's procedure for requests from the WAN (Facts 76 and 77) in order to use Susaki, which is directed to requests from the LAN (Fact 72). Again, if one skilled in the art were to have combined Susaki and Shitama (which Appellants do not admit would have been obvious), one skilled in the art would have added the LAN security disclosed by Susaki to the WAN security disclosed by Shitama.

A claimed feature is thus missing even after the references are combined, and such feature would not otherwise have been known or obvious so as to support a 35 U.S.C. §103(a) rejection in accordance with *KSR* and the U.S. Patent and Trademark Office Examination Guidelines for Determining Obviousness under 35 U.S.C. §103 in view of *KSR*. Therefore, even if Susaki and Shitama were combined as suggested in the Office Action (which Appellants do not admit would have been obvious), the combination of Susaki and Shitama would not allow a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN as recited in claims 1, 11 and 20.

4. Summary

Because the combination of Susaki and Shitama fails to discuss determining whether requests come in from the WAN or the LAN as defined by independent claims 1 and 11, and because the combination of Susaki and Shitama fails to handle requests from both the WAN and the LAN as defined by independent claims 1, 11 and 20 as discussed above, Susaki and Shitama fail to disclose or suggest all of the features of independent claims 1, 11 and 20. Moreover, the claimed features that are missing from Susaki and Shitama would not otherwise have been known or obvious.

B. Susaki And Shitama Fail To Suggest Demanding A Determination Only For Requests That Involve Real-Time Processing As Required By Dependent Claims 7 And 16

Dependent claim 7 recites a controller that demands the user of the communication device to determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing, which is a specified request from the WAN (Fact 82). Dependent claim 16 likewise recites that the user of the communication device must determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing, which is a specified request from the WAN (Fact 83). Appellants did not previously raise this argument.

Page 4 of the Office Action refers to Susaki's col. 9, lines 42-48 as disclosing this feature (Fact 85). Appellants disagree (Fact 86) because col. 9, lines 42-48 fail to discuss predetermined online real-time processing (Facts 87-89), e.g., fail to suggest requiring approval from a user if the request involves predetermined online real-time processing. Shitama fails to overcome the deficiencies of Susaki because Shitama likewise fails to discuss predetermined online real-time processing (Fact 90).

C. Dependent Claims

Claims 2-10 and 12-19 depend either directly or indirectly from one of claims 1 and 11. Claims 2-10 and 12-19 are thus patentable at least for their

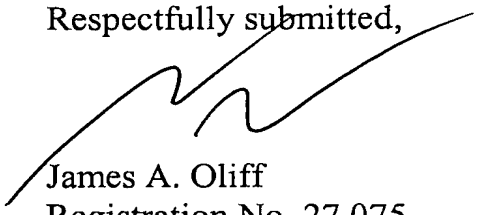
dependency from claim 1 or claim 11, as well as for the additional features they recite.

X. CONCLUSION

For all of the reasons discussed above, it is respectfully submitted that the rejections are in error and that claims 1-20 are in condition for allowance.

For all of the above reasons, Appellants respectfully request this Honorable Board to reverse the rejections of claims 1-20.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Scott M. Schulte
Registration No. 44,325

JAO:SMS/mef

OLIFF & BERRIDGE, PLC
P.O. Box 320850
Alexandria, Virginia 22320-4850
Telephone: (703) 836-6400
Fax: (703) 836-2787
Email: email@oliff.com

Filed: February 27, 2009

XI. APPENDIX A - CLAIMS SECTION

1. (Rejected) A communication device, comprising:

a first input portion connected with a wide area network (WAN);

a second input portion connected with a local area network (LAN); and

a controller that:

determines whether a request to perform predetermined processing came in from the WAN or the LAN;

automatically accepts an operation according to the request every time that it is determined that the request came in from the LAN;

allows a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN; and

allows the predetermined processing to be performed according to the request when a performance of the operation according to the request is accepted.

2. (Rejected) The communication device according to claim 1, wherein the controller includes an IP address table storage portion that stores IP addresses of terminals connected with the LAN, and the controller identifies a terminal which has issued the request with reference to the IP address indicating the terminal and the IP address table.

3. (Rejected) The communication device according to claim 1, further comprising:

a display unit that displays an inquiry about whether the performance of the operation according the request is accepted or rejected; and

an input unit through which the user can input an answer of whether the request is accepted or rejected in response to the inquiry.

4. (Rejected) The communication device according to claim 3, wherein the display unit and the input unit are provided at an operating portion.

5. (Rejected) The communication device according to claim 1, wherein the controller informs a terminal, which made the request, that the user of the communication device is not near the communication device when the determination is not made by the user within a predetermined period of time.

6. (Rejected) The communication device according to claim 1, wherein the controller demands a user of a LAN terminal to determine whether the performance of the operation according to the request is accepted or rejected when it is determined that the request came in from the WAN.

7. (Rejected) The communication device according to claim 1, wherein the controller demands the user of the communication device to determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing, which is a specified request from the WAN.

8. (Rejected) The communication device according to claim 1, wherein the controller:

exclusively sets a first operation mode in which the determination of whether the performance of the operation is accepted or rejected is demanded; and

sets a second operation mode in which the controller allows the predetermined processing to be performed according to the request that comes in from the WAN when the performance of the operation is accepted aside from the first operation mode.

9. (Rejected) The communication device according to claim 1, wherein the controller informs a WAN terminal, that made the request, of a result of the determination by the user of the communication device as to the performance of the operation.

10. (Rejected) The communication device according to claim 1, wherein the request received from the LAN or the WAN is at least one of: performance of a printing operation, transmission of facsimile data, reading of data from detachably attachable memory, setting change of device, and reading of received facsimile data, and the controller performs processing in accordance with the received request.

11. (Rejected) A method of communicating with a communication device, comprising:

a first input portion connected with a wide area network (WAN);

a second input portion connected with a local area network (LAN), comprising:

determining whether a request to perform predetermined processing came in from the WAN or the LAN;

automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN;

allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN; and

allowing the predetermined processing to be performed according to the request when a performance of the operation according to the request is accepted.

12. (Rejected) The method of claim 11, further comprising:

identifying a terminal which has issued the request with reference to an IP address indicating the terminal and an IP address table.

13. (Rejected) The method of claim 11, further comprising:

displaying an inquiry about whether the performance of the operation according the request is accepted or rejected; and

inputting a user answer of whether the request is accepted or rejected in response to the inquiry.

14. (Rejected) The method of claim 11, further comprising:

informing a terminal, which made the request, that the user of the communication device is not near the communication device when the determination is not made by the user within a predetermined period of time.

15. (Rejected) The method of claim 11, wherein a user of a LAN terminal must determine whether the performance of the operation according to the request is accepted or rejected when it is determined that the request came in from the WAN.

16. (Rejected) The method of claim 11, wherein the user of the communication device must determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing, which is a specified request from the WAN.

17. (Rejected) The method of claim 11, further comprising:

setting, exclusively, a first operation mode in which the determination of whether the performance of the operation is accepted or rejected is demanded; and

setting a second operation mode in which the controller allows the predetermined processing to be performed according to the request that comes in from the WAN when the performance of the operation is accepted aside from the first operation mode.

18. (Rejected) The method of claim 11, further comprising:

informing a WAN terminal, that made the request, of a result of the determination by the user of the communication device as to the performance of the operation.

19. (Rejected) The method of claim 11, wherein the request received from the LAN or the WAN is at least one of: performance of a printing operation, transmission of facsimile data, reading of data from detachably attachable memory, setting change of device, and reading of received facsimile data, and processing is performed in accordance with the received request.

20. (Rejected) A communication device, comprising:

a first input portion connected with a wide area network (WAN);

a second input portion connected with a local area network (LAN); and

a controller that:

automatically performs predetermined processing according to a request every time that a performance of an operation is requested by a LAN;

allows a user of the communication device to determine whether an operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN; and

performs predetermined processing according to a request from the WAN when a performance of the operation according to the request is accepted.

XII. APPENDIX B - CLAIM SUPPORT AND DRAWING ANALYSIS SECTION

1. A communication device **{communication device 1, Fig. 1}**, comprising:

a first input portion connected with a wide area network (WAN) **{WAN port 6, Fig. 2}**;

a second input portion connected with a local area network (LAN) **{LAN port 7, Fig. 2}**; and

a controller **{CPU 39, Fig. 2}** that:

determines whether a request to perform predetermined processing came in from the WAN or the LAN **{step S2, Fig. 3, paragraph [0038]}**;

automatically accepts an operation according to the request every time that it is determined that the request came in from the LAN **{step S2: NO, step S8, Fig. 3, paragraphs [0050] and [0051]}**;

allows a user of the communication device **{communication device 1, Fig. 1}** to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN **{step S2: YES, step S5, Fig. 2; steps S21-S24, Fig. 4, Fig. 6, paragraphs [0041] - [0043] and [0051]}**; and

allows the predetermined processing to be performed according to the request **{for example, a printing operation, paragraphs**

[0045], [0060] and [0061]} when a performance of the operation according to the request is accepted **{step S2: NO, step S7: YES, step S8, Fig. 3}**.

7. The communication device **{communication device 1, Fig. 1}** according to claim 1, wherein the controller **{CPU 39, Fig. 2}** demands the user of the communication device **{communication device 1, Fig. 1}** to determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing **{S3, Fig. 3, paragraph [0040]}**, which is a specified request from the WAN **{S2: YES, Fig. 3, paragraph [0040]}**.

11. A method of communicating with a communication device **{communication device 1, Fig. 1}**, comprising:

a first input portion connected with a wide area network (WAN) **{WAN port 6, Fig. 2}**;

a second input portion connected with a local area network (LAN) **{LAN port 7, Fig. 2}**, comprising:

determining whether a request to perform predetermined processing came in from the WAN or the LAN **{step S2, Fig. 3, paragraph [0038]}**;

automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN **{step S2: NO, step S8, Fig. 3, paragraphs [0050] and [0051]}**;

allowing a user of the communication device {**communication device 1, Fig. 1**} to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN {**step S2: YES, step S5, Fig. 2; steps S21-S24, Fig. 4, Fig. 6), paragraphs [0041] - [0043] and [0051]**}; and

allowing the predetermined processing to be performed according to the request {**for example, a printing operation, paragraphs [0045], [0060] and [0061**} when a performance of the operation according to the request is accepted {**step S2: NO, step S7: YES, step S8, Fig. 3**}.

16. The method of claim 11, wherein the user of the communication device {**communication device 1, Fig. 1**} must determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing {**S3, Fig. 3, paragraph [0040]**}, which is a specified request from the WAN {**S2: YES, Fig. 3, paragraph [0040]**}.

20. A communication device {**communication device 1, Fig. 1**}, comprising:

a first input portion connected with a wide area network (WAN) {**WAN port 6, Fig. 2**};

a second input portion connected with a local area network (LAN) {**LAN port 7, Fig. 2**}; and

a controller {**CPU 39, Fig. 2**} that:

automatically performs predetermined processing according to a request every time that a performance of an operation is requested by a LAN {**step S2: NO, step S8, Fig. 3, paragraphs [0050] and [0051]**};

allows a user of the communication device {**1**} to determine whether an operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN {**step S2: YES, step S5, Fig. 2; steps S21-S24, Fig. 4, Fig. 6), paragraphs [0041] - [0043] and [0051]**}; and

performs predetermined processing according to a request {**for example, a printing operation, paragraphs [0045], [0060] and [0061**} from the WAN when a performance of the operation according to the request is accepted {**step S2: NO, step S7: YES, step S8, Fig. 3**}.

XIII. APPENDIX C - MEANS OR STEP PLUS FUNCTION ANALYSIS SECTION

NONE

XIV. APPENDIX D - EVIDENCE SECTION

A copy of each of the following items of evidence relied on by the Appellant and/or the Examiner in this appeal is attached:

Table of Contents

Page

Application, filed September 29, 2003 51

Final Rejection, mailed September 3, 2008 78

Request for Reconsideration, filed December 2, 2008 93

Advisory Action, mailed December 23, 2008 100

Susaki et al., U.S. Patent No. 6,189,032 103

Shitama, U.S. Patent Application Publication No 2002/0110123 129

Joubert et al., U.S. Patent No. 6,101,616 142

Allen et al., U.S. Patent Application Publication No. 2003/0041333 157

Boehmke et al., U.S. Patent Application Publication No. 2002/0126822 177

COMMUNICATION DEVICE CONNECTED TO A LOCAL AREA NETWORK AND WIDE AREA NETWORK AND METHOD THEREOF

BACKGROUND OF THE INVENTION

1. Field of Invention

[0001] The invention relates to a communication device that is connected to a LAN (local area network) and/or a WAN (wide area network) and can perform a printing operation in accordance with a print request made by LAN terminals and/or WAN terminals through the LAN and/or WAN.

2. Description of Related Art

[0002] Japanese Laid-Open Patent Publication No. 2002-91739 (page 4 and Figure 1) and Japanese Laid-Open Patent Publication No. 08-30692 (page 5 and Figure 1) disclose a printing system in which a printer is connected to a LAN and/or a WAN. U.S. Patent Application Publication No. US 2002/0042884 (page 4 and Figure 1) discloses a printing system in which an authenticated document is printed at a distant location by remote control.

[0003] A system has been suggested in which a printer is connected with a WAN, such as the Internet, as well as personal computers installed in a building or a house, via a LAN. In this system, the printer can be used by specific computers by performing authentication using, for example, passwords. However, this authentication confirms the identity of not only users on the WAN but also users on the LAN, so that this system has less usability. Also, a password may be artificially leaked to outsiders as well as being leaked by stealing packets from a network (sniffing). Accordingly, there is a possibility that unauthorized users can use the printer by using stolen passwords.

SUMMARY OF THE INVENTION

[0004] The invention thus provides a communication device that prevents unauthorized access by outsiders while improving its usability. According to one exemplary aspect of the invention, a communication device, which is connected to a wide area network (WAN) and a local area network (LAN), includes a controller that determines whether a request to perform predetermined processing came in from the WAN or the LAN, allows a user of the communication device to determine whether an operation according to the request is accepted or rejected when it is determined that the request came in from the WAN, and allows the predetermined processing to be performed according to the request when a performance of the operation according to the request is accepted.

[0005] According to the communication device, the user of the communication device determines whether the performance of an operation according to the request is accepted or rejected every time the request for the performance of the processing is made to the communication device through the WAN. Thus, unauthorized access by outsiders can be prevented. When a request is made to the communication device through the LAN, processing according to the request is performed without requesting the user of the communication device to perform the determination, thereby improving the usability of the communication device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Embodiments of the invention will be described in detail with reference to the following figures wherein:

[0007] FIG. 1 shows a usage pattern of a communication device to which the invention is applied;

[0008] FIG. 2 is a block diagram showing an electronic configuration of the communication device of the embodiment;

[0009] FIG. 3 is a flowchart outlining command receiving processing executed by the communication device;

[0010] FIG. 4 is a flowchart outlining acceptance/rejection determining processing performed in the command receiving processing;

[0011] FIG. 5 is an explanatory diagram showing an operating condition of the communication device during the acceptance/rejection determining processing;

[0012] FIG. 6 is a flowchart outlining acceptance/rejection determining processing performed in a command receiving processing according to another embodiment;

[0013] FIG. 7 is a flowchart outlining processing to be executed by a PC in accordance with the acceptance/rejection determining processing of FIG. 6; and

[0014] FIG. 8 is an explanatory diagram showing an operating condition of the PC during the acceptance/rejection determining processing.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0015] Embodiments of the invention will be described with reference to the accompanying drawings. As shown in FIG. 1, a communication device 1 includes a line control unit 3 and a communication module 5. The line control unit 3 includes an external port 4 (FIG. 2), which is connected with an analog line L1 (a telephone line made of 2-wire cord or 4-wire cord) that is connected to a telephone port of a splitter 8 installed inside

buildings, such as houses and offices. The communication module 5 includes a WAN port 6 and a LAN port 7 (FIG. 2). The WAN port 6 is connected to a wide-area network (WAN), such as the Internet, via a LAN cable L3, an ADSL modem 9, a LAN cable L2, and the splitter 8, in this order.

[0016] The LAN port 7 is connected with a hub 11. The hub 11 is connected to various LAN terminals, for example, bidirectionally communicable PCs (personal computers) 13, 14, a network printer (such as an ink-jet printer or a laser-beam printer) 16, an IP telephone 15 that can send and receive voice signals in an IP (Internet Protocol) system, and an Internet facsimile machine 17. That is, the hub 11 is connected with a local-area network (LAN) constructed by the LAN terminals 13 to 17 installed in a building.

[0017] The splitter 8 is a well-known splitter used for an ADSL (asymmetric digital subscriber line). The splitter 8 separates a superimposed transmission signal into a first signal and a second signal to output the first signal and the second signal to the telephone port and the ADSL modem port, respectively. The first signal is a signal of a maximum of about 4 kHz, which is transmitted from a splitter (not shown) installed in a base station. The second signal is a signal for ADSL, having a higher frequency than the first signal. The splitter 8 also superimposes one signal on another, which are inputted from the telephone port and the ADSL modem port, and transmits the superimposed signal to the splitter in the base station.

[0018] That is, the communication device 1 of the embodiment can connect subscriber telephones in public switched telephone networks (PSTN) by using the line control unit 3. In addition, the communication device 1 can connect the Internet, such as a WAN, via the communication module 5 and the ADSL modem 9. The communication device 1 also serves as a router that routes data (IP packet) to be transmitted and received between a communication device (e.g. a WWW server) on the Internet and the LAN terminals 13 to 17 on the LAN, in accordance with control executed by a router control unit 101 of the communication module 5.

[0019] The communication device 1 of the embodiment has a print function and a copy function as well as a common facsimile function of optically reading an image from a document, converting image data representing the image into facsimile data, sending the facsimile data via the analog line L1, receiving facsimile data transmitted through the analog line L1, and forming an image on a recording sheet according to the received facsimile data.

[0020] The print function refers to a function of forming an image onto a recording sheet according to code data transmitted from the PC 13 or 14 or a word processor. Upon

receipt of code data from an external PC via a PC interface (I/F) 24 or from the PC 13 or 14 on the LAN via the communication module 5, the communication device 1 forms an image onto a recording sheet according to the data. The copy function refers to a function of making a copy of an image on a recording sheet according to image data read from a document by a scanning unit 35 and a recording unit 37.

[0021] Next, an electronic configuration of the communication device 1 will be described. As shown in FIG. 2, the communication device 1 includes a CPU 39, a ROM 81, a RAM 83, the scanning unit 35, an encoder 85, the recording unit 37, a decoder 87, operation keys 270, an LCD (liquid crystal display) 274, a modem 89, the line control unit 3, the PC interface (I/F) 24, a mail control unit 91, and a function extension interface 93, which are connected with each other via a bus 95. The function extension interface 93 is connected with the communication module 5.

[0022] The CPU 39 is a brain of the communication device 1 and executes centralized control of the communication device 1. For example, the CPU 39 reads a control program from the ROM 81 to execute a facsimile data transmitting/receiving operation and a printing operation in accordance with the control program.

[0023] The ROM 81 stores a print function program group to permit the communication device 1 to operate as a facsimile machine. More specifically, for example, the ROM 81 stores a data receiving program for forming an image by the recording unit 37 according to facsimile data received by the line control unit 3 from an external facsimile machine, as the facsimile function program. In addition, the ROM 81 stores a print function program group to permit the communication device 1 to operate as a printer that prints data transmitted from a PC through a WAN or a LAN. More specifically, for example, the ROM 81 stores a PC print program for forming an image by the recording unit 37 according to data, which is received by the communication module 5 from the PC 13 or 14 on the LAN or a PC on a WAN, by analyzing a command coming in from the outside. Further, the ROM 81 stores a recording unit control program to be called up in the PC print program, other various programs and various data required during execution of the various programs. The RAM 83 serves as a work memory to be used when various controls are executed, a data storage area for storing data, such as facsimile data, to be transmitted or received, and a table storage area for storing a table of IP addresses assigned to the PCs 13, 14 on the LAN.

[0024] The scanning unit 35 scans and reads a document in order to transmit facsimile data or make a copy of the document. The encoder 85 performs an encoding

operation to convert image data read by the scanning unit 35 into encoded image data in G3 format (facsimile format) and then outputs the image data. The decoder 87 decodes the image data in the facsimile format to convert the data into image data processible in the recording unit 37. The recording unit 37 functions as a so-called color laser-beam printer that can form an image in color onto a recording unit, as described above. The recording unit 37 prints a color image onto a recording sheet according to image data decoded by the decoder 37 and outputs the recording sheet having the image thereon after the printing operation is completed, in accordance with instructions provided from the CPU 39 that runs the recording unit control program.

[0025] The operation keys 270 are provided at an upper portion of an operating panel 27. The operation keys 270 input a command signal into the CPU 39 to perform various operations, in accordance with instructions given by a user of the communication device 1. The LCD 274, as a display unit, is also provided at the operating panel 27 and displays various messages to show operating procedures and to inform errors to the user. The LCD 274 also functions as a touch-sensitive panel in order to display one-touch keys thereon when input from the user is required and in order to input instructions given by the user into the CPU 39.

[0026] The modem 89 is provided so that the line control unit 3 can transmit and receive facsimile data to and from an external facsimile machine connected to a public network, via the splitter 8. The line control unit 3 sends a dial signal to the public network and answers a ringing signal from the public network. For example, the line control unit 3 allows the communication device 1 to be communicable with the external facsimile machine.

[0027] The PC interface 24 is used to connect a PC and the communication device 1 via a parallel cable so that the communication device 1 can receive code data from the PC. The mail control unit 91 realizes transmitting and receiving of facsimile data using electronic mail by transmitting and receiving electronic mail to and from an external communication device connected to the Internet. A handset (H/S) 26 is connected with the modem 89 via the line control unit 3. The function extension interface 93 is a serial interface, such as AIO (analog input and output) or RS232C, that can detachably connected with the communication module 5, which includes the separate-type router control unit 101.

[0028] The communication module 5 includes the router control unit 101, the hub 103, an IP telephone unit 105, a wireless communication unit 107, a Web printing unit 110, and an interface connection terminal 109 which connects with the router control unit 101.

The communication module 5 is connected with the function extension interface 93 via the interface connection terminal 109.

[0029] The router control unit 101, which functions as a broadband router having a well-known IP Masquerade (Network Address Port Translation) function and a routing function, transmits and receives IP packets, via the ADSL modem 9, to and from a communication device on the Internet. That is, the router control unit 101 mutually translates a private IP (Internet Protocol) address used in the LAN and a global IP address used in the WAN (the Internet in this embodiment) by the IP Masquerade function, and bidirectionally communicably connects the PCs 13, 14 on the LAN with a communication device on the WAN (WWW server) by the routing function.

[0030] For example, the router control unit 101 bidirectionally communicably connects the IP telephone unit 105, the wireless communication unit 107, and the Web printing unit 110 with the Internet, via the ADSL modem 9, by transmitting and receiving data to and from the IP telephone unit 105, the wireless communication unit 107, the Web printing unit 110 via the hub 103.

[0031] Further, the router control unit 101 bidirectionally communicably connects the LAN terminals 13 to 17 with the Internet by performing communication with the LAN terminals 13 to 17 on the LAN connected with the LAN port 7 via the hub 103. That is, for example, the router control unit 101 provides routing and then transmits data, which is received from the WWW server on the Internet, to the addressed LAN terminals 13 to 17.

[0032] The router control unit 101 can conduct communication with the CPU 39 of the communication device 1 via the function extension interface 93. That is, the LAN terminals 13 to 17, the IP telephone unit 105, the wireless communication unit 107, and the Web printing unit 110 can bidirectionally communicate with the CPU 39 of the communication unit 1 via the router control unit 101 and the function extension interface 93. For example, upon receipt of code data for printing from the PC 13 or 14 on the LAN through the router control unit 101, the CPU 39 of the communication device 1 runs the print function program. Then, the CPU 39 calls the recording unit control program during the execution of the print function program to control the recording unit 37 to form an image based on the data.

[0033] The IP telephone unit 105, which is connected with the router control unit 101 via the hub 103, contains a voice signal into an IP packet and conducts voice communication (telephone conversation) with an external IP telephone through the Internet.

The wireless communication unit 107 conducts wireless communication between the communication device 1 and an external communication device. By using a wireless connection technology, such as the Bluetooth Standard (a standard for short-range wireless communication) or the IrDA Standard (a standard for infrared wireless communication), the external wireless communication device can be bidirectionally communicably connected with each unit of the communication device 1. That is, in the communication device 1, the LAN terminals 13 to 17 can be connected with the communication device 1 by using a cable via the LAN port 7 connected to the hub 103. By using the wireless communication unit 107, the LAN terminals 13 to 17 can be connected with the communication device 1 without cables or wires.

[0034] The Web printing unit 110 includes a CPU 111, a ROM 113, a RAM 115 and a network interface 117. The Web printing unit 110 connects itself with the Internet and communicates with the CPU 39 of the communication device 1 by performing communication with the router control unit 101 via the network interface 117.

[0035] The ROM 113 of the Web printing unit 110 stores a Web print function program group for performing operations for capturing data from the WWW server and for printing data downloaded from the WWW server by the recording unit 37 of the communication device 1. The ROM 113 also stores flag information representing operating conditions of the communication device 1 when the Web print function is being executed.

[0036] More particularly, the Web print unit 110 has a print function, a data memory function, a data transfer function, a log memory function, and an error display function. The print function is to allow the recording unit 37 to print an image based on data downloaded from the WWW server through the router control unit 101. The data memory function is to temporarily store data in the RAM 115. The data transfer function includes two types of the data transfer function: one of which is to transfer downloaded data, via the LAN port 7, to the printer 16 of the transfer target connected to the LAN, and another of which is to transfer downloaded data, via the LAN port 7, to the PC 13 or 14 connected with the LAN. The log memory function is to store log information of each processing performed by the Web printing unit 110. The error display function is to display error messages on the LCD 274. These functions are implemented by the Web printing function program group and each function is implemented based on flag information (that is, on/off of the function).

[0037] Basically, users of the LAN terminals 13 to 17 can access the communication device 1 without restraint. On the other hand, for outside users, who use

WAN terminals, the access to the communication device 1 is restricted to persons who have the authority. That is, there are three types of people as outside users: people who have a password and a user ID to use the communication device 1, people who are allowed to use the communication device 1 in certain conditions although they do not have a password, and people who do not have any authority to access the communication device 1 under any circumstances. In this embodiment, as described above, the communication device 1 is protected from unauthorized outside users through the WAN.

[0038] Next, an operation of the communication device 1 will be described. FIG. 3 is a flowchart of an example of the command receiving processing performed by the communication device 1. Upon receipt of a command (step 1, hereinafter, S stands for step) (at this point, it is unknown whether the command was come in through the LAN or the WAN), the CPU 111 of the communication module 5 determines whether the command came in through the WAN (S2). This determination is performed based on, for example, an IP address of a transmitter that has sent the command. The communication module 5 is also assigned an IP address, so that the LAN terminals 13 to 17 and WAN terminals can access the communication device 1 by using the IP address of the communication module 5.

[0039] When the command comes in through the WAN (S2:YES), the CPU 111 then determines whether the command is a request to perform processing as a predetermined online real-time processing (S3). The command for online real-time processing will be described in detail later. For example, when the command is a real-time print command, the CPU 111 makes an affirmative judgment (S3:YES), and when the command is a storage print command, the CPU 11 makes a negative judgment (S3:NO).

[0040] When the received command is a command for performing online real-time processing, such as the real-time print command (S3:YES), the CPU 111 determines whether a current operation mode is set to a user authentication mode or an automatic authentication mode (S4). The user authentication mode is a mode in which a user identifies an access source without performing a password authentication and determines whether the access is acceptable, every time an access is made from a WAN terminal. The automatic authentication mode is a mode in which a password authentication is automatically performed by the communication device 1 and an access from a WAN terminal is accepted only when the inputted password is authenticated.

[0041] When the current operation mode is a user authentication mode (S4:YES), an acceptance/rejection determining processing shown in FIG. 4 is performed (S5). As

shown in FIG. 4, at the acceptance/rejection determining processing, the user is informed that the access has been being made from the WAN terminal (S21). At that time, as shown in FIG. 5, sounds come out of a speaker 271 to indicate that an access has been made from the WAN terminal at the present time.

[0042] In addition, a screen that allows a user to determine whether the request is acceptable is displayed on the LCD 274 (S22). For example, as shown in FIG. 5, a message such that "A request made by Mr./Ms. *** has come in." is displayed on the LCD 274. Words "accept" and "reject" are also displayed on the LCD 274 so as to indicate which operation keys 270B, 270C function as an acceptance key and a rejection key. "***" is specified based on a user registration table, which is created in advance to provide a relationship between users of WAN terminals and IP addresses of the WAN terminals. When an IP address of an WAN terminal accessing to the communication device 1 is not registered in the user registration table in advance, the IP address is displayed on the LCD 274, just as it is. A type of a print request is displayed on the LCD 274 with the messages or IP address, corresponding to the requested command, such as a real-time print command or a storage print command.

[0043] When the determination of acceptance/rejection is made by the user within a predetermined period of time (S23:YES) and "acceptance" is selected by the user by pressing the acceptance key 270B (S24:YES), the acceptance of the request is determined (S25). Then, this determination result is sent back to the main routine (the command receiving processing) of FIG. 3. For example, when the command is a print request, the acceptance of printing is determined.

[0044] At S24, when "rejection" is selected by the user by pressing the rejection key 270C (S24:NO), the rejection of the request is determined (S26). Then, this determination result is sent back to the main routine (the command receiving processing) of FIG. 3. At S23, when the determination is not made by the user within the predetermined period of time (S23:NO), a user absent flag is set (S27) and then this information is sent back to the main routine (the command receiving processing) of FIG. 3.

[0045] Referring to FIG. 3, when a user absent flag is not set (S6:NO) and the CPU 11 receives the acceptance of the request (S7:YES), the CPU 111 performs processing in accordance with the data received with the command (S8). For example, when the command is a print request, the CPU 111 allows the recording unit 37 to perform a printing operation based on received print data. As described above, the execution of the printing operation is

determined in accordance with the determination by the user (the acceptance/rejection of the request), even when the print data is transmitted from a WAN terminal, without performing the password authentication.

[0046] When receiving the rejection of the request (S7:NO), the CPU 111 informs the WAN terminal user, which has accessed, through the WAN, that the request has been rejected (S11). For example, when the command is a print request, the printing operation requested by the WAN terminal is not performed in the communication device 1 and the user of the WAN terminal is informed that the printing operation cannot be performed. An acceptance of the request or a completion of processing may be also informed to the user of the WAN terminal (access source), when processing is performed by the acceptance of the request.

[0047] At S6, when the user absent flag is on (S6:YES), the CPU 111 informs the WAN terminal, which has accessed, of the absence of the user, through the WAN (S10). For example, when the command is a print request, the printing operation requested by the WAN terminal is not performed in the communication device 1 and the user of the WAN terminal is informed that the printing operation cannot be performed because the user of the communication device 1 who has the authority to perform authentication was not present near the communication device 1.

[0048] At S4, when the current operation mode is an automatic authentication mode (S4:NO), the password authentication is automatically performed by the communication device 1 (S9). At the password authentication, a password and a user ID transmitted from a WAN terminal together with the command are confirmed whether the password and the user ID match those registered in the communication device in advance. When the transmitted password and user ID match the registered ones, an affirmative judgment is made at S7 (S7:YES). When the transmitted password and user ID do not match the registered ones, a negative judgment is made at S7 (S7:NO) and then the CPU 111 informs the WAN terminal that the request cannot be performed in the communication device (S11).

[0049] At S3, when it is determined that the command is the storage print command (S3:NO), that is, the command is not an online real-time processing command, the CPU 111 temporarily stores print data received together with the command, into the RAM 115. Then, the printing operation is performed by the recording unit 37 by confirming the stored print data by the user, printing and erasing the print data.

[0050] At S2, when it is determined that the command came in through the LAN (S2:NO), flow moves to S8 and the CPU 111 immediately performs processing corresponding to the command. For example, when the command is a print request, the CPU 111 allows the recording unit 37 to perform the printing operation.

[0051] According to the communication device 1 of the above-described embodiment, the user of the communication device 1 must determine whether a request from a WAN terminal is accepted or rejected every time the request comes in through a WAN. Accordingly, unauthorized access to the communication device 1 from an external Internet can be prevented. When a request is made by any of the LAN terminals 13 to 17, processing is immediately performed without performing the determination/selection by the user. Thus, the usability of the communication device 1 can be improved.

[0052] Next, another embodiment of the invention will be described. The structure of a communication device and command receiving processing according to this embodiment are the same as the structure of the communication device 1 shown in FIGS. 1 and 2 and the command receiving processing of FIG. 3, respectively. Therefore, only different parts will be described below.

[0053] FIG. 6 shows a flowchart of acceptance/rejection determining processing included in the command receiving processing according to another embodiment. As shown in FIG. 6, at the acceptance/rejection determining processing of this embodiment, first, a command to allow a user of a predetermined PC 13 to determine acceptance or rejection of the request through the LAN port 7 and the LAN (S31).

[0054] FIG. 7 shows a flowchart of processing to be executed by a PC 13 in accordance with the acceptance/rejection determining processing (S31). As shown in FIG. 7, upon receipt of the command (S41), the PC 13 displays a dialog box for allowing the user to determine "acceptance" or "rejection", on its display (S42). For example, as shown in FIG. 8, a message (a dialog box 20A) such that "A request made by Mr./Ms. *** has come in." is displayed on the display of the PC 13. In addition, operation buttons 20B and 20C, which indicate "Yes" and "No", respectively, are displayed so as to be clicked by using a mouse. At that time, as shown in FIG. 8, sounds come out of a speaker (not shown) to inform the user of the communication device 1 that an access is being made from a WAN terminal.

[0055] After that, when the user of the PC 13 accepts the access by clicking the "yes" button 20B (S43:YES), the acceptance of the request is determined (S44) and then the determination result is sent back to the communication device 1 via the LAN (S45). When

the user of the PC 13 rejects the request by clicking the "no" button 20C (S43:NO), the rejection of the request is determined (S46) and then this determination result is sent back to the communication device 1.

[0056] As shown in FIG. 6, upon receipt of the determination result from the PC 13 (S32), the CPU 111 determines whether the reply was received within a predetermined period of time (S33). When the CPU 111 receives the reply from the PC 13 within a predetermined period of time (S33:YES), then, the CPU 111 determines whether the reply (determination result) is acceptance of the request (S34). When the reply is the acceptance of the request (S34:YES), the acceptance of the request is determined (S35) and then this determination result is sent back to the main routine (the command receiving processing) of FIG. 3.

[0057] At S33, when the CPU 111 does not receive the reply within the predetermined period of time (S33:NO), the CPU 111 sets a PC user absent flag on (S37). This information is sent back to the main routine (the command receiving processing) of FIG. 3. At S34, when the CPU 111 receives the rejection of the request from the PC 13 (S34:NO), the rejection of the request is determined (S36) and then this determination result is sent back to the main routine (command receiving processing) of FIG. 3.

[0058] According to the communication device 1 of this embodiment, the predetermined PC 13 is demanded, via the LAN, to determine whether a request is accepted or rejected every time a request comes in through the WAN. Accordingly, unauthorized access to the communication device 1 from an external Internet can be prevented. When a request is made by any of the LAN terminals 13 to 17, processing is immediately performed without performing the determination by the PC 13. Thus, the usability of the communication device 1 can be improved.

[0059] While the invention has been described in detail with reference to the specific embodiments thereof, it should be apparent to those skilled in the art that various changes, arrangements and modifications may be applied therein without departing from the spirit and scope of the invention.

[0060] In the above-described embodiments, the print function has been described as an example of the invention. The processing, which is the same as the above-described embodiments, may be applied to, for example, a case where access is made to the communication device 1 from a WAN terminal in order to read and store data from and into the RAM 83 or a case where access is made to the communication device 1 from a WAN terminal in order to change the setting of the communication device 1 by remote control.

When the communication device 1 is designed so as to be detachably attachable with a portable memory card, the processing, which is the same as the above-described embodiments, may be applied to a case where access is made to the memory card from a WAN terminal in order to read and store data from and into the memory card. Further, the processing, which is the same as the above-described embodiments, may be applied to a case where transmission of facsimile data is started by remote control by a WAN terminal or a case where a WAN terminal reads received facsimile data by accessing the communication device 1.

[0061] In the above cases, the data transmission by the facsimile function, the reading of data from the memory card, the setting of the communication device 1 by remote control, and the viewing received facsimile data correspond to the online real-time processing, so that an affirmative judgment is made at S3 of FIG. 3 upon receipt of these commands. Voice messages and recording of data into the memory card are examples of commands other than the online real-time processing, so that a negative judgment is made at S3 of FIG. 3 upon receipt of these command.

[0062] A network printer is one of preferable examples of the communication device 1. However, the communication device 1 may be, for example, a multifunctional printer that has a facsimile function, a copy function and an e-mail transmitting and receiving function. When the WAN port 6 and the LAN port 7 are separately provided, it can be determined whether the data is transmitted from a LAN terminal or a WAN terminal, by determining signals outputted from the ports 6, 7. The WAN includes an Integrated Services Digital Network (ISDN), a Switched Multimegabit Data Service (SMDS), a frame relay, a High data rate Digital Subscriber Line (HDSL), an Asynchronous Transfer Mode (ATM) line, and a general telephone line, as well as the Internet.

[0063] According to the communication device 1 described in each embodiment above, unauthorized access from outsiders can be prevented because a user of the communication device 1 must determine whether a request is accepted every time the request is made by a WAN terminal. When a request is made by a LAN terminal, the determination is not requested to the user, so that the usability of the communication device 1 can be improved. When a request is come in through the LAN, the LAN terminal, which is an access source and has made the request, can be specified with reference to the user registration table.

[0064] As described above, the communication device 1 includes the LCD 284 and the operation keys 270. With this structure, the user who can directly operate the communication device 1 can determine and select whether the request of the WAN terminal is accepted. Because the LCD.274 and the operation keys 270 are provided to the operating panel 27, the user can directly operate the operating panel 27 as a user interface.

[0065] In the communication device 1, the CPU 111 informs an access source of a user's absence from the communication device 1 when the user does not operate the communication device 1 within the predetermined period of time. With this structure, when the user does not reply to the request made by a WAN terminal, the user's absence from the communication device 1 can be informed to the WAN terminal of the access source. When it is determined that a request is made by a WAN terminal, a user of a LAN terminal must determine whether the request is accepted or rejected. Accordingly, even when the user of the communication device 1 does not exist near the communication device 1, the determination can be made on the request of the WAN terminal via the LAN. Only when a predetermined online real-time processing is requested by a WAN terminal, the acceptance/rejection determination is demanded to the user. Therefore, the communication device 1 can immediately perform the processing requested by the WAN terminal.

[0066] Further, according to the communication device 1, the user authentication mode and the automatic authentication mode can be set. In the user authentication mode, the acceptance/rejection determination is demanded to the user without fail when a request is made by a WAN terminal. In the automatic authentication mode, for example, a password authentication is performed to permit the execution of a request by a WAN terminal. As described above, an appropriate mode can be exclusively set in accordance with usage of the communication device 1. When a request made by a WAN terminal is rejected by the user of the communication device 1 or the PC 13, this determination result can be informed to the WAN terminal. Furthermore, the communication device 1 can implement processing corresponding to a command, which is issued by a LAN terminal and a WAN terminal, wherein the command is for performing an printing operation, transmitting facsimile data, reading data from detachably attachable memory, changing the setting of the communication device 1, or reading received facsimile data.

WHAT IS CLAIMED IS:

1. A communication device connected with a wide area network (WAN) and a local area network (LAN), comprising:

a controller that:

determines whether a request to perform predetermined processing came in from the WAN or the LAN;

allows a user of the communication device to determine whether an operation according to the request is accepted or rejected when it is determined that the request came in from the WAN; and

allows the predetermined processing to be performed according to the request when a performance of the operation according to the request is accepted.

2. The communication device according to claim 1, wherein the controller includes an IP address table storage portion that stores IP addresses of terminals connected with the LAN, and the controller identifies a terminal which has issued the request with reference to the IP address indicating the terminal and the IP address table.

3. The communication device according to claim 1, further comprising:

a display unit that displays an inquiry about whether the performance of the operation according the request is accepted or rejected; and

an input unit through which the user can input an answer of whether the request is accepted or rejected in response to the inquiry.

4. The communication device according to claim 3, wherein the display unit and the input unit are provided at an operating portion.

5. The communication device according to claim 1, wherein the controller informs a terminal, which made the request, that the user of the communication device is absent near the communication device when the determination is not made by the user within a predetermined period of time.

6. The communication device according to claim 1, wherein the controller demands a user of a LAN terminal to determine whether the performance of the operation according to the request is accepted or rejected when it is determined that the request came in from the WAN.

7. The communication device according to claim 1, wherein the controller demands the user of the communication device to determine whether the performance of the operation according to the request is accepted or rejected only when the received request

involves predetermined online real-time processing, which is a specified request from the WAN.

8. The communication device according to claim 1, wherein the controller:

exclusively sets a first operation mode in which the determination of whether the performance of the operation is accepted or rejected is demanded; and

sets a second operation mode in which the controller allows the predetermined processing to be performed according to the request that comes in from the WAN when the performance of the operation is accepted aside from the first operation mode.

9. The communication device according to claim 1, wherein the controller informs a WAN terminal, that made the request, of a result of the determination by the user of the communication device as to the performance of the operation.

10. The communication device according to claim 1, wherein the request received from the LAN or the WAN is at least one that requests performance of a printing operation, transmission of facsimile data, reading of data from detachably attachable memory, setting change of device, and reading of received facsimile data, and the controller performs processing in accordance with the received request.

11. A method of communicating with a wide area network (WAN) and a local area network (LAN) connected to a communication device, comprising:

determining whether a request to perform predetermined processing came in from the WAN or the LAN;

allowing a user of the communication device to determine whether an operation according to the request is accepted or rejected when it is determined that the request came in from the WAN; and

allowing the predetermined processing to be performed according to the request when a performance of the operation according to the request is accepted.

12. The method of claim 11, further comprising:

identifying a terminal which has issued the request with reference to an IP address indicating the terminal and an IP address table.

13. The method of claim 11, further comprising:

displaying an inquiry about whether the performance of the operation according the request is accepted or rejected; and

inputting a user answer of whether the request is accepted or rejected in response to the inquiry.

14. The method of claim 11, further comprising:

informing a terminal, which made the request, that the user of the communication device is absent near the communication device when the determination is not made by the user within a predetermined period of time.

15. The method of claim 11, wherein a user of a LAN terminal must determine whether the performance of the operation according to the request is accepted or rejected when it is determined that the request came in from the WAN.

16. The method of claim 11, wherein the user of the communication device must determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing, which is a specified request from the WAN.

17. The method of claim 11, further comprising:

setting, exclusively, a first operation mode in which the determination of whether the performance of the operation is accepted or rejected is demanded; and

setting a second operation mode in which the controller allows the predetermined processing to be performed according to the request that comes in from the WAN when the performance of the operation is accepted aside from the first operation mode.

18. The method of claim 11, further comprising:

informing a WAN terminal, that made the request, of a result of the determination by the user of the communication device as to the performance of the operation.

19. The method of claim 11, wherein the request received from the LAN or the WAN is at least one that requests performance of a printing operation, transmission of facsimile data, reading of data from detachably attachable memory, setting change of device, and reading of received facsimile data, and processing is performed in accordance with the received request.

20. A communication device connected with a wide area network (WAN) and a local area network (LAN), comprising:

a controller that:

automatically performs predetermined processing according to a request when a performance of an operation is requested by a LAN;

allows a user of the communication device to determine whether an operation according to the request is accepted or rejected when it is determined that the request came in from the WAN; and

performs predetermined processing according to a request from the WAN when a performance of the operation according to the request is accepted.

ABSTRACT OF THE DISCLOSURE

A communication device is connected with a wide area network (WAN) and a local area network (LAN) and includes a recording unit that performs predetermined processing in accordance with a request, that comes in through the WAN or the LAN. A controller of a communication module of the communication device determines whether a request came in through the WAN or the LAN. When the request comes in through the WAN, the controller demands an acceptance/rejection determination as to the performance of the request from a user of the communication device. When the performance of the requested operation is accepted, the controller performs the processing according to the request that came in through the WAN.

FIG.1

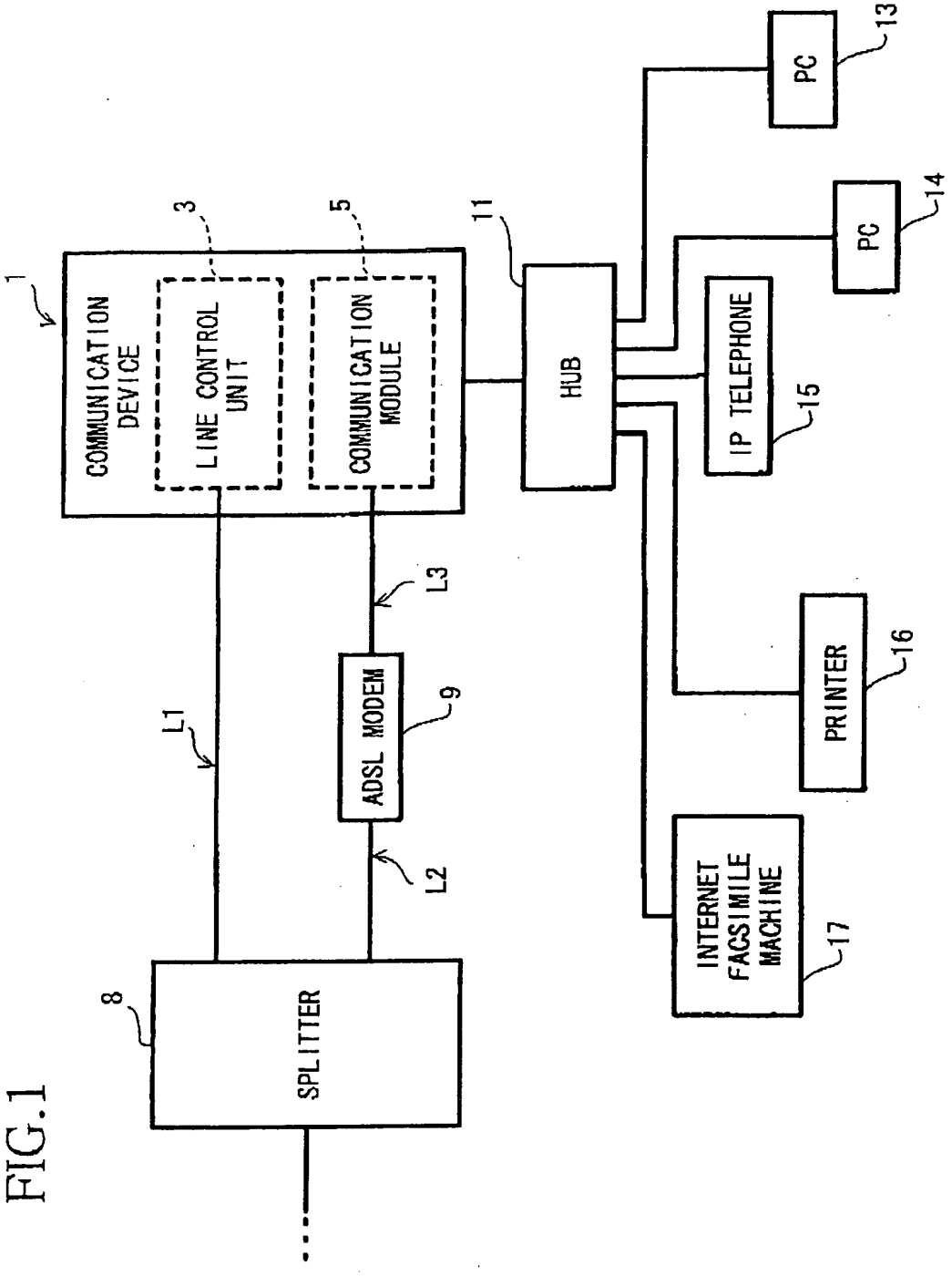

1
COMMUNICATION DEVICE
3
LINE CONTROL UNIT
5
COMMUNICATION MODULE
11
HUB
PC
13
PC
14
IP TELEPHONE
15
PRINTER
16
INTERNET FACSIMILE MACHINE
17
L1
L2
L3
ADSL MODEM
9
8
SPLITTER

FIG.2

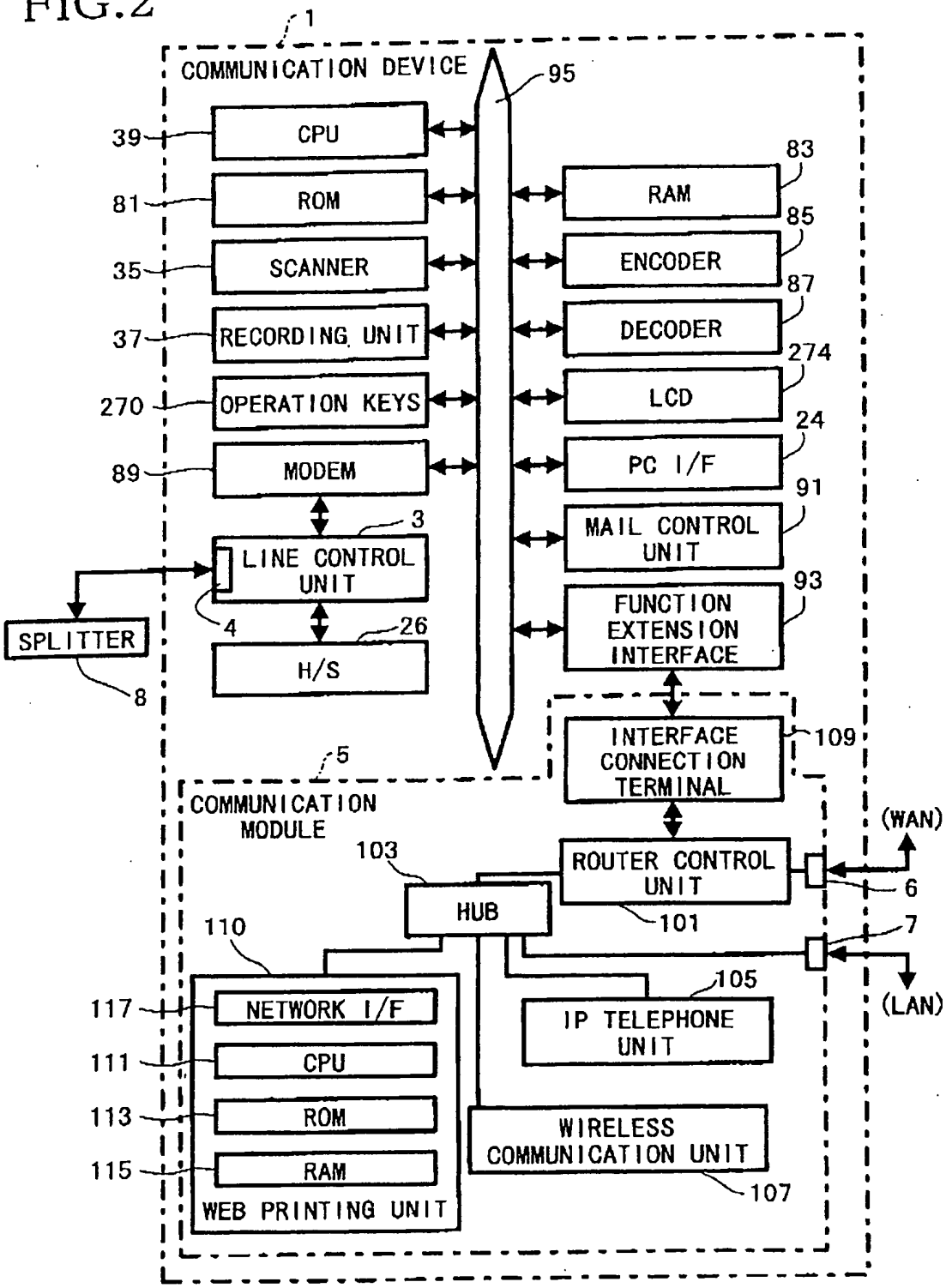

1
COMMUNICATION DEVICE
95
39
CPU
81
ROM
35
SCANNER
37
RECORDING UNIT
270
OPERATION KEYS
89
MODEM
3
LINE CONTROL UNIT
4
26
H/S
SPLITTER
8
83
RAM
85
ENCODER
87
DECODER
274
LCD
24
PC I/F
91
MAIL CONTROL UNIT
93
FUNCTION EXTENSION INTERFACE
109
INTERFACE CONNECTION TERMINAL
5
COMMUNICATION MODULE
103
ROUTER CONTROL UNIT
101
HUB
110
(WAN)
6
7
(LAN)
105
IP TELEPHONE UNIT
117
NETWORK I/F
111
CPU
113
ROM
115
RAM
WEB PRINTING UNIT
WIRELESS COMMUNICATION UNIT
107

FIG.3

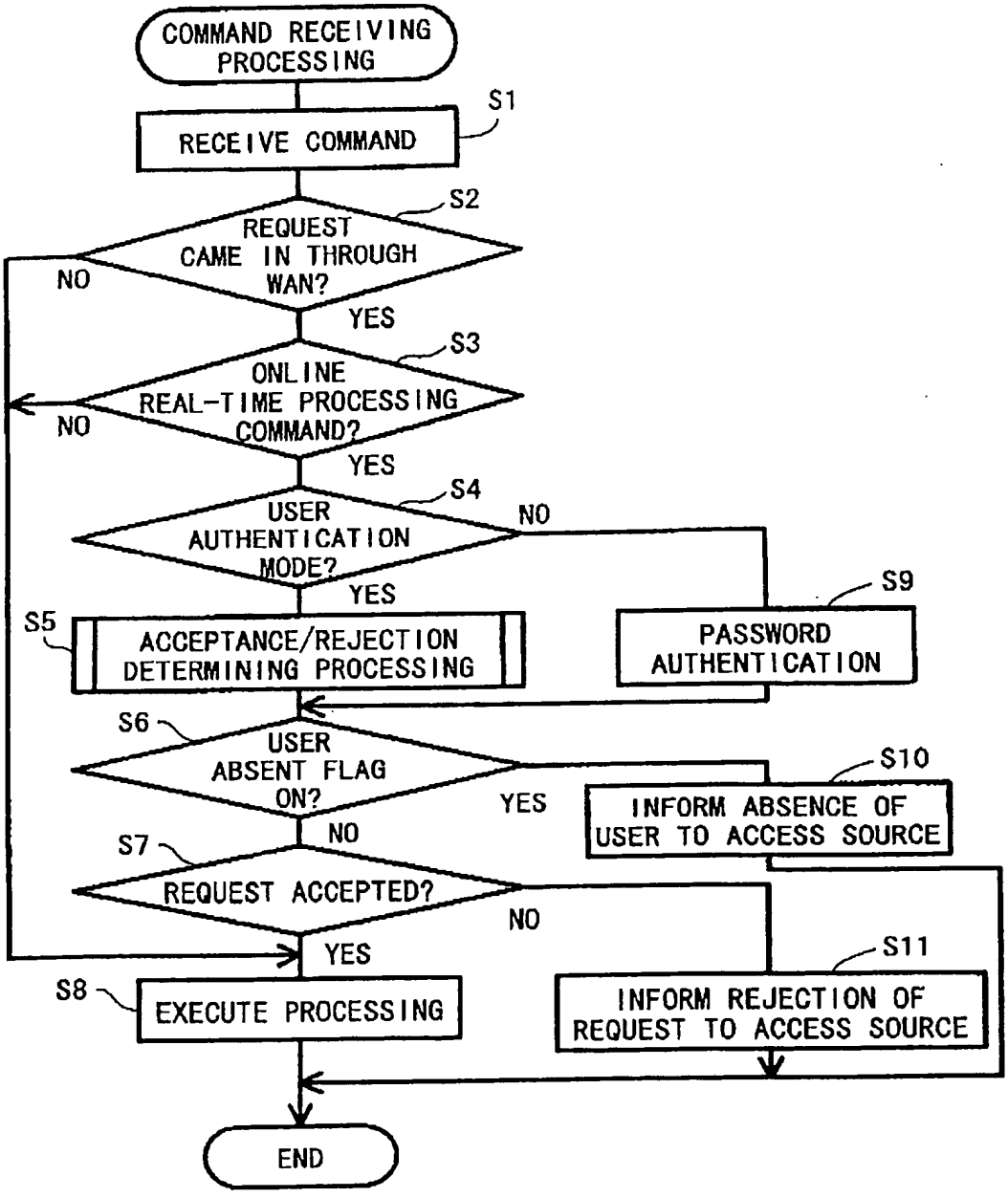
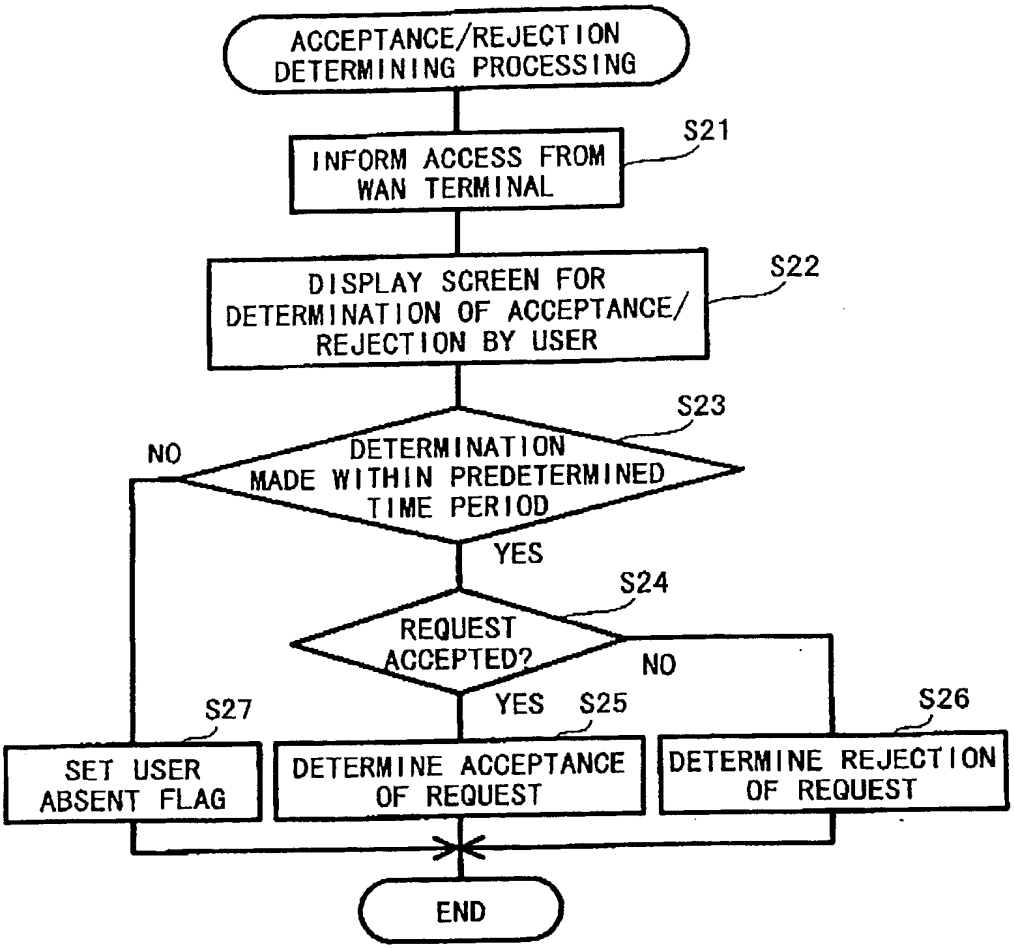

COMMAND RECEIVING PROCESSING
S1
RECEIVE COMMAND
S2
REQUEST CAME IN THROUGH WAN?
NO
YES
S3
ONLINE REAL-TIME PROCESSING COMMAND?
NO
YES
S4
USER AUTHENTICATION MODE?
NO
YES
S5
ACCEPTANCE/REJECTION DETERMINING PROCESSING
S9
PASSWORD AUTHENTICATION
S6
USER ABSENT FLAG ON?
YES
S10
INFORM ABSENCE OF USER TO ACCESS SOURCE
NO
S7
REQUEST ACCEPTED?
NO
YES
S8
EXECUTE PROCESSING
S11
INFORM REJECTION OF REQUEST TO ACCESS SOURCE
END

FIG.4


ACCEPTANCE/REJECTION DETERMINING PROCESSING
INFORM ACCESS FROM WAN TERMINAL
S21
DISPLAY SCREEN FOR DETERMINATION OF ACCEPTANCE/ REJECTION BY USER
S22
S23
DETERMINATION MADE WITHIN PREDETERMINED TIME PERIOD
NO
YES
S24
REQUEST ACCEPTED?
NO
YES
S25
S26
S27
SET USER ABSENT FLAG
DETERMINE ACCEPTANCE OF REQUEST
DETERMINE REJECTION OF REQUEST
END

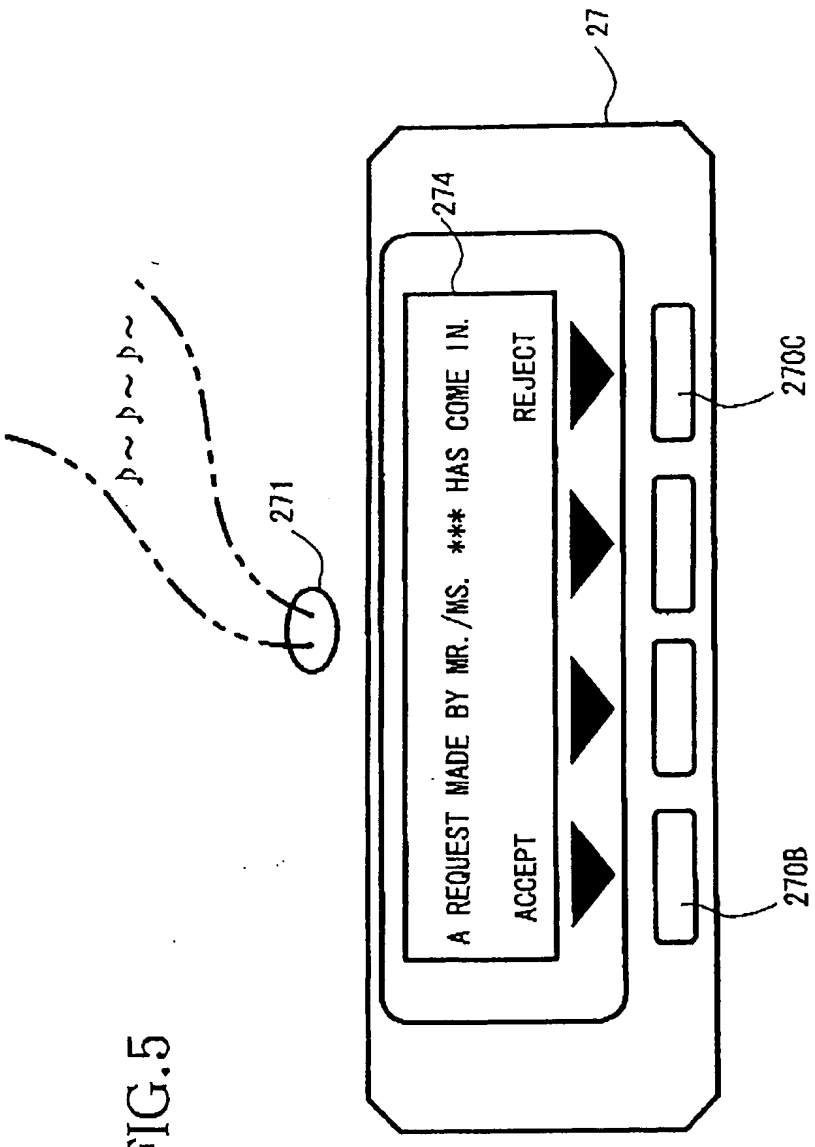

27
274
A REQUEST MADE BY MR./MS. *** HAS COME IN.
ACCEPT
REJECT
270C
270B
271

FIG.5

FIG.6

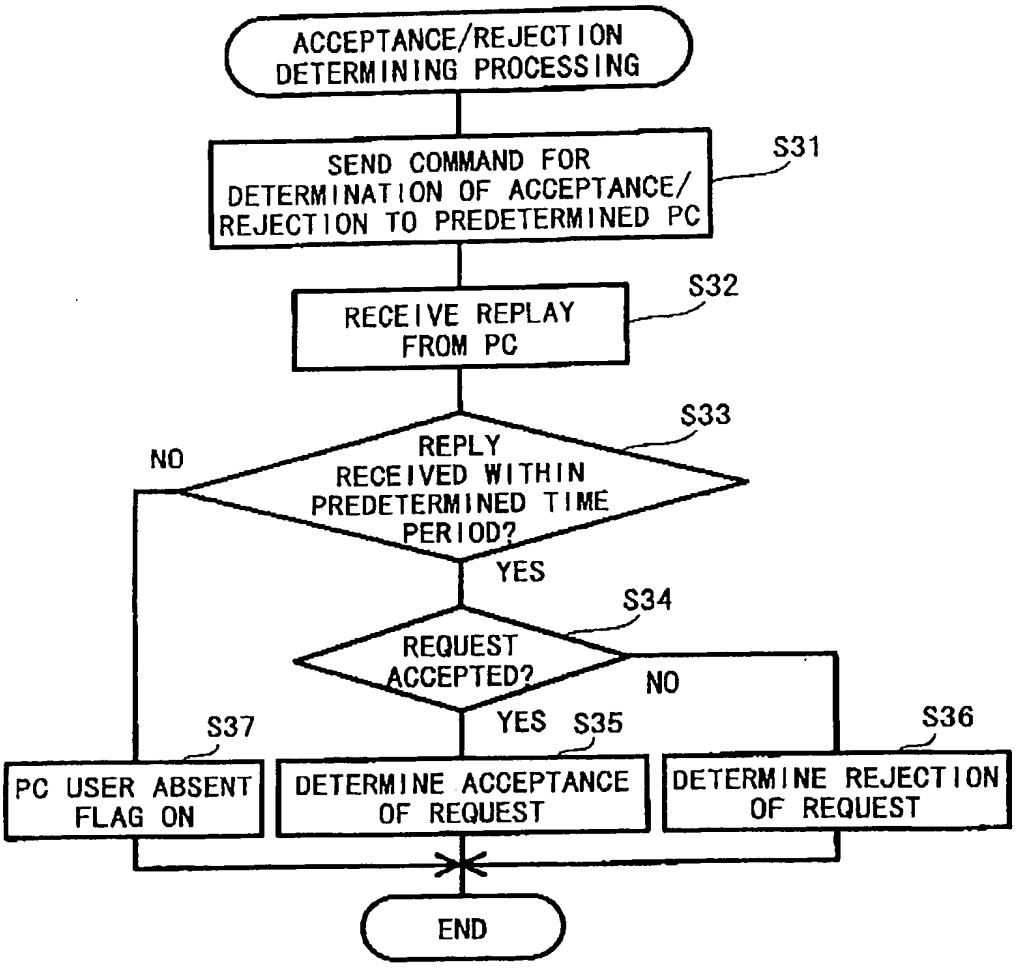

ACCEPTANCE/REJECTION DETERMINING PROCESSING
SEND COMMAND FOR DETERMINATION OF ACCEPTANCE/ REJECTION TO PREDETERMINED PC
S31
RECEIVE REPLAY FROM PC
S32
REPLY RECEIVED WITHIN PREDETERMINED TIME PERIOD?
S33
NO
YES
REQUEST ACCEPTED?
S34
NO
YES
S35
S36
S37
PC USER ABSENT FLAG ON
DETERMINE ACCEPTANCE OF REQUEST
DETERMINE REJECTION OF REQUEST
END

FIG.7

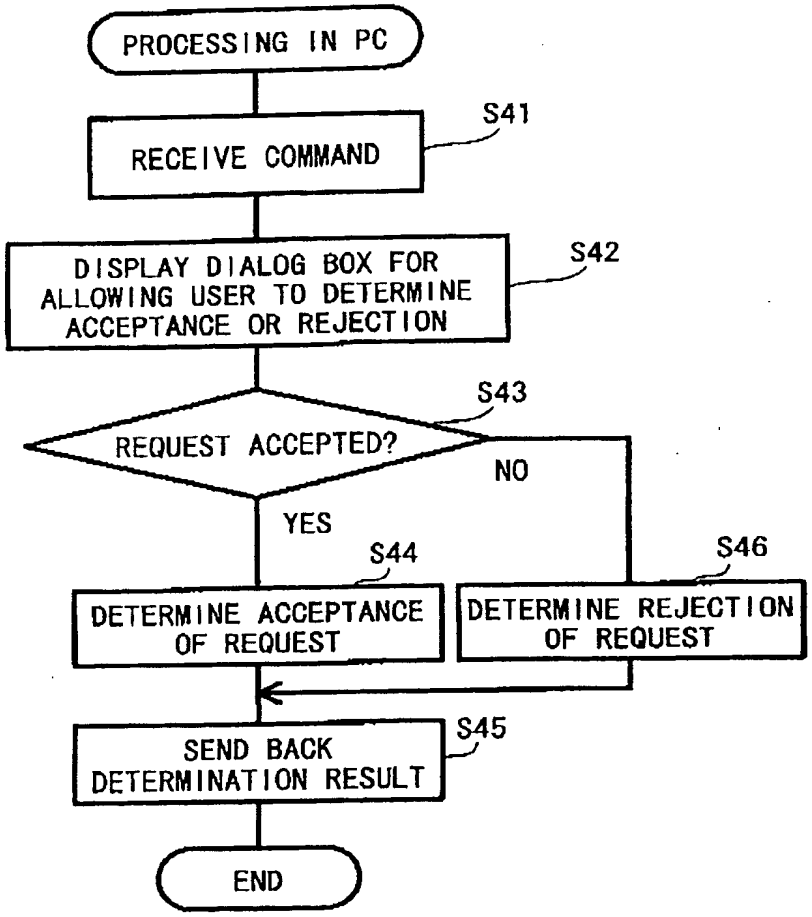
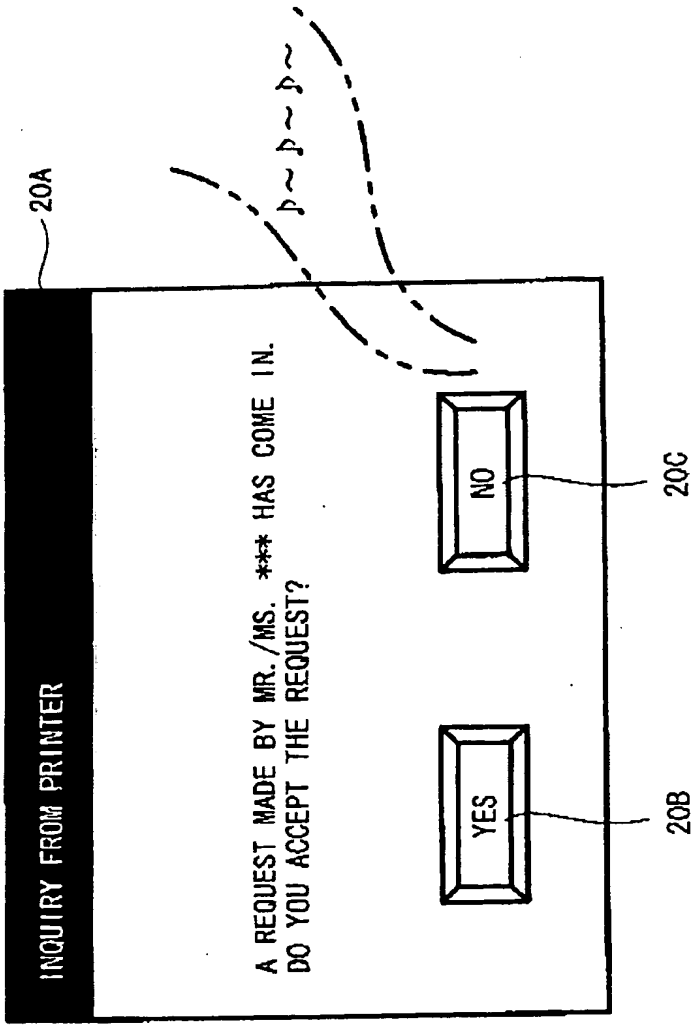

PROCESSING IN PC
RECEIVE COMMAND
S41
DISPLAY DIALOG BOX FOR ALLOWING USER TO DETERMINE ACCEPTANCE OR REJECTION
S42
REQUEST ACCEPTED?
S43
NO
YES
S44
S46
DETERMINE ACCEPTANCE OF REQUEST
DETERMINE REJECTION OF REQUEST
SEND BACK DETERMINATION RESULT
S45
END

FIG.8


20A
INQUIRY FROM PRINTER
A REQUEST MADE BY MR./MS. *** HAS COME IN.
DO YOU ACCEPT THE REQUEST?
YES
NO
20B
20C

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/671,686	09/29/2003	Kazuma Aoki	117025	1077

25944 7590 09/03/2008

OLIFF & BERRIDGE, PLC
P.O. BOX 320850
ALEXANDRIA, VA 22320-4850

RECEIVED
SEP - 5 2008
OLIFF & BERRIDGE

EXAMINER	
KEEFER, MICHAEL E	
ART UNIT	PAPER NUMBER
2154	
MAIL DATE	DELIVERY MODE
09/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

FINAL REJECTION/
NOTICE OF APPEAL

DUE DATE
DEC - 5 2008

DOCKETED
By BRJ on Sep. 5 2008
and
By Fmp on 9/5 2008
Oliff & Berridge

DOCKETED
By BRJ on Sep. 5 2008
and
By Fmp on 9/5 2008
Oliff & Berridge

Office Action Summary	Application No.	Applicant(s)	
	10/671,686	AOKI ET AL.	
	Examiner	Art Unit	
	MICHAEL E. KEEFER	2154	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5/14/2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responsive to the Amendment filed 5/14/2008.

Claim Rejections - 35 USC § 103

1. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

2. Claims 1, 3, 6-7, 9, 11, 13, 15-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Susaki et al. (US 6189032 B1), hereafter Susaki in view of Shitama (US 2002/0110123).

Regarding **claims 1, 3, 6, and 9**, Susaki discloses:

A communication device (Fig. 1, server 2) connected with a wide area network (WAN) and a local area network (LAN) (communication network 3), comprising:

a controller (see Fig. 3) that:

determines whether a request to perform predetermined processing came in from the WAN or the LAN; (Col 9, Lines 38-48 describes the process of the controller determining whether a request requires the approval of another user)

allows a user of the communication device to determine whether an operation according to the request is accepted or rejected when it is determined that the request came in from the WAN (Col. 10, Lines 1-7 describe how a user is allowed to determine whether a request is allowed or rejected) ; and

allows the predetermined processing to be performed according to the request when a performance of the operation according to the request is accepted. (Col 10, lines 7-9 and 14-18 state that the request is granted and made to process if the request is granted by the other user)

a display unit that displays an inquiry about whether the performance of the operation according the request is accepted or rejected (See display unit 23 in Fig. 3); and

an input unit through which the user can input an answer of whether the request is accepted or rejected in response to the inquiry. (See input unit 24 in Fig. 3)

wherein the display unit and the input unit are provided at an operating portion. (It is inherent that the display and input units must be in an operating portion, or else they would not function as disclosed by Susaki.)

the controller demands a user of a LAN terminal to determine whether the performance of the operation according to the request is accepted or rejected when it is determined that the request came in from the WAN. (Col. 10, Lines 1-7 describe how a user is allowed to determine whether a request is allowed or rejected)

wherein the controller demands the user of the communication device to determine whether the performance of the operation according to the request is accepted or rejected only when the received request

involves predetermined online real-time processing, which is a specified request from the WAN. (Col. 9 lines 42-48 disclose that not only is a user's authority taken into account when determining if a demand for approval is made to a user, but also the type of the request.)

wherein the controller:

exclusively sets a first operation mode in which the determination of whether the performance of the operation is accepted or rejected is demanded; and

sets a second operation mode in which the controller allows the predetermined processing to be performed according to the request that comes in from the WAN when the performance of the operation is accepted aside from the first operation mode. (Note in Fig. 5 it is disclosed that the operation mode can be changed by changing the access limits for a particular service or services to either require another user to approve the request, or to automatically allow the request. See Col. 7, lines 65-67 and Col. 8 lines 1-9)

the controller informs a WAN terminal, that made the request, of a result of the determination by the user of the communication device as to the performance of the operation. (Fig. 11, items 3014 and/or 3018 both inform the requestor of the disposition of the request.)

Therefore, Susaki discloses all the limitations of claims 1, 3, 4, 6-7, and 9 except for the selection criteria specifically being whether a user is

located on a LAN or a WAN and that all LAN requests are allowed to proceed automatically.

The general concept of determining whether requests come from a LAN or WAN, as well as the concept of automatically allowing all requests from a LAN are well known in the art as taught by Shitama. ([0052], it is determined that request came from the WAN by determining what interface the request came from, and additionally by determining the IP address associated with the request in [0053], further, Shitama generally teaches that greater security is needed when handling requests that originate from a WAN, whereas all requests from the LAN are trusted, Note at least paragraph 11, which discusses limiting and authorizing requests from a WAN, but implicitly allows all local requests for local resources.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Susaki with the general concept of determining whether requests come from a LAN or WAN, and applying stricter security criteria to requests from a WAN as taught by Shitama.

Regarding **claims 11, 13, and 15-18**, Susaki discloses:

A method of communicating with a wide area network (WAN) and a local area network (LAN) connected to a communication device, comprising:

determining whether a request to perform predetermined processing came in from the WAN or the LAN; (Col 9, Lines 38-48

describes determining whether a request requires the approval of another user)

allowing a user of the communication device to determine whether an operation according to the request is accepted or rejected when it is determined that the request came in from the WAN (Col. 10, Lines 1-7 and 14-18 describe how a user is allowed to determine whether a request is allowed or rejected); and

allowing the predetermined processing to be performed according to the request when a performance of the operation according to the request is accepted. (Col 10, lines 7-9 state that the request is granted and made to process if the request is granted by the other user)

displaying an inquiry about whether the performance of the operation according the request is accepted or rejected; (Fig. 15 shows the display of an inquiry) and

inputting a user answer of whether the request is accepted or rejected in response to the inquiry. (Because in Col 10, lines 7-9 state that the client terminal sends back approval information, it must have been input at some time, via a button on the dialog in Fig. 15. Also see Col. 11, lines 56-62.)

wherein a user of a LAN terminal must determine whether the performance of the operation according to the request is accepted or rejected when it is determined that the request came in from the WAN.

(Col. 10, Lines 1-7 describe how a user is allowed to determine whether a request is allowed or rejected)

wherein the user of the communication device must determine whether the performance of the operation according to the request is accepted or rejected only when the received request involves predetermined online real-time processing, which is a specified request from the WAN. (Col. 9 lines 42-48 disclose that not only is a user's authority taken into account when determining if a demand for approval is made to a user, but also the type of the request.)

setting, exclusively, a first operation mode in which the determination of whether the performance of the operation is accepted or rejected is demanded; and

setting a second operation mode in which the controller allows the predetermined processing to be performed according to the request that comes in from the WAN when the performance of the operation is accepted aside from the first operation mode. (Note in Fig. 5 it is disclosed that changing the access limits for a particular service or services to either require another user to approve the request, or to automatically allow the request can change the operation mode. See Col. 7, lines 65-67 and Col. 8 lines 1-9)

informing a WAN terminal, that made the request, of a result of the determination by the user of the communication device as to the

performance of the operation. (Fig. 11, items 3014 and/or 3018 both inform the requestor of the disposition of the request.)

Therefore, Susaki discloses all the limitations of claims 11, 13, 15, and 18 except for the selection criteria specifically being whether a user is located on a LAN or a WAN.

The general concept of determining whether requests come from a LAN or WAN, as well as the concept of automatically allowing all requests from a LAN are well known in the art as taught by Shitama. ([0052], it is determined that request came from the WAN by determining what interface the request came from, and additionally by determining the IP address associated with the request in [0053], further, Shitama generally teaches that greater security is needed when handling requests that originate from a WAN, whereas all requests from the LAN are trusted, Note at least paragraph 11, which discusses limiting and authorizing requests from a WAN, but implicitly allows all local requests for local resources.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Susaki with the general concept of determining whether requests come from a LAN or WAN, and applying stricter security criteria to requests from a WAN as taught by Shitama.

Regarding **claim 20**, Susaki discloses:

A communication device connected with a wide area network (WAN) and a local area network (LAN), comprising:

a controller that:

automatically performs predetermined processing according to a request when a performance of an operation is requested by a LAN (Col. 9 lines 57-67 disclose that if a client is in a group that does not require approval the request is automatically granted);

allows a user of the communication device to determine whether an operation according to the request is accepted or rejected when it is determined that the request came in from the WAN (Col. 10, Lines 1-7 and 14-18 describe how a user is allowed to determine whether a request is allowed or rejected); and

performs predetermined processing according to a request from the WAN when a performance of the operation according to the request is accepted. (Col 10, lines 7-9 states that the request is granted and made to process if the other user grants the request.)

Therefore, Susaki discloses all the limitations of claim 20 except that the defining characteristic of the two groups is their presence on a LAN or a WAN.

The general concept of determining whether requests come from a LAN or WAN, as well as the concept of automatically allowing all requests from a LAN are well known in the art as taught by Shitama. ([0052], it is determined that request came from the WAN by determining what interface the request came from, and additionally by determining the IP address associated with the request in [0053], further, Shitama generally

teaches that greater security is needed when handling requests that originate from a WAN, whereas all requests from the LAN are trusted, Note at least paragraph 11, which discusses limiting and authorizing requests from a WAN, but implicitly allows all local requests for local resources.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Susaki with the general concept of determining whether requests come from a LAN or WAN as taught by Shitama.

3. Claims 2 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Susaki and Shitama as applied to claims 1 and 11 above, and further in view of Joubert et al. (US 6101616), hereafter Joubert.

Susaki and Shitama teach all the limitations of **claims 2 and 12** except for an IP address table used to differentiate between terminals.

The general concept of using IP addresses to identify terminals on a network is well-known in the art as taught by Joubert (Col. 2, lines 22-25 teach that a table is used to correspond IP addresses to terminal MAC addresses for unique identification, further, lines 30-36 teach that terminals should use their IP address in LAN communications and that unique terminals can be identified by using a table to look up a correspondence between an IP address and a unique MAC address).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Susaki and Shitama with the general

concept of using IP addresses to identify terminals on a network as taught by Joubert in order to be more robust.

4. Claims 5 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Susaki and Shitama as applied to claims 1 and 11 above, and further in view of Allen et al. (US 2003/0041333 A1), hereafter Allen.

Susaki and Shitama teach all of the limitations of **claims 5 and 14** except for the requester being notified if the authorization request times out.

The general concept of notifying a requester if a request times out is well-known in the art as taught by Allen ("the user rejecting the request or not accepting the request within an established time interval a pre-recorded video greeting is sent" Abstract lines 5-7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Susaki and Shitama with the teaching of notifying a requester if a request times out as taught by Allen in order to increase user efficiency.

5. Claims 10 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Susaki and Shitama as applied to claims 1 and 11 above, and further in view of Boehmke et al. (US 2002/0126822 A1) hereafter Boehmke.

Susaki discloses that a server provides "services" but does not specifically define them.

Susaki and Shitama teach all the limitations of **claims 10 and 19** except for that the request received from the LAN or the WAN is at least one of: performance of a printing operation, transmission of facsimile data,

reading of data from detachably attachable memory, setting change of device, and reading of received facsimile data, and processing is performed in accordance with the received request. Susaki merely teaches that the server provides "services".

The general concept of a server being able to provide printing and facsimile related services is well-known in the art as taught by Boehmke ([0062] teaches that a server may transmit data to one or more peripheral devices such as printers and facsimiles, among others).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Susaki and Shitama with the teaching of a server being able to provide printing and facsimile related services as taught by Boehmke in order to make the server more versatile.

Response to Arguments

6. Applicant's arguments filed 5/14/2008 have been fully considered but they are not persuasive.

7. Applicant argues that because Susaki includes different levels of authorization, a combination of Susaki and Shitama would not automatically accept all requests from the LAN. While Applicant's statements about Susaki including different possible user levels is correct, it does not hold that all of the levels of scrutiny must be used in a combination with Shitama. In fact, as the Examiner has stated in the above rejection of the independent claims (1, 11, and 20) above, Shitama teaches that scrutiny only needs to be applied to requests that emanate from the WAN, whereas requests from the LAN are always fulfilled.

Therefore, in a combination with Susaki, one of ordinary skill in the art at the time of the invention would place all LAN address as having a user authority level of '0' in the table of Fig. 5 (i.e. 'Always processable').

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL E. KEEFER whose telephone number is (571)270-1591. The examiner can normally be reached on Monday through Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MEK 8/28/2008

/Joseph E. Avellino/
Primary Examiner, Art Unit 2146

PATENT APPLICATION

RESPONSE UNDER 37 CFR §1.116
EXPEDITED PROCEDURE
TECHNOLOGY CENTER ART UNIT 2154

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Kazuma AOKI et al. Group Art Unit: 2154

Application No.: 10/671,686 Examiner: M. KEEFER

Filed: September 29, 2003 Docket No.: 117025

For: COMMUNICATION DEVICE PREVENTING UNAUTHORIZED ACCESS TO ITS SERVICES VIA USER INTERVENTION AND A METHOD THEREOF

REQUEST FOR RECONSIDERATION AFTER FINAL REJECTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In reply to the September 3, 2008 Office Action, reconsideration of the above-identified application is respectfully requested in light of the following remarks. Claims 1-20 are pending in this application.

Claims 1, 3, 6, 7, 9, 11, 13, 15-18 and 20 were rejected under 35 U.S.C. §103(a) over Susaki et al. (Susaki), U.S. Patent No. 6,189,032, in view of Shitama, U.S. Publication No. 2002/0110123. The rejection is respectfully traversed.

Applicants explain below why the combination of Susaki and Shitama fails to disclose or suggest the processing of requests that come in from the LAN and the WAN as defined in the independent claims.

DETERMINING BETWEEN REQUESTS FROM THE WAN AND THE LAN

Claim 1 calls for a controller that determines whether a request to perform predetermined processing came in from the WAN or the LAN; and claim 11 calls for the step of determining whether a request to perform predetermined processing came in from the WAN or the LAN.

Susaki fails to disclose this feature because Susaki fails to discuss the WAN, and Shitama treats requests that come in from the WAN and the LAN the same.

Susaki discloses a client server system where a terminal 1 and a server 2 are connected through a communication network 3 such as a LAN (Fig. 1 and col. 5, lines 8-12). Susaki fails to provide any mention with regard to the WAN, and col. 9, lines 38-48 cited on page 2 of the Office Action fails to mention the WAN.

Shitama merely disclose a device that receives data from a WAN and transmits the data to the LAN. Therefore, even if Susaki and Shitama were combined as suggested in the Office Action (which Applicants do not admit would have been obvious), data from the WAN would be transmitted to the LAN, and would be processed the same as if the data came in from the LAN. Therefore, the combination of Susaki and Shitama would not need to determine whether requests come in from the WAN or the LAN, or need to determine whether a request to perform predetermined processing came in from the WAN or the LAN as called for by claims 1 and 11, for the additional processing called for by claims 1, 11 and 20.

REQUESTS FROM THE LAN

Claim 1 calls for a controller that automatically accepts an operation according to the request every time that it is determined that the request came in from the LAN; claim 11 calls for the step of automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN; and claims 20 calls for a controller that

automatically performs predetermined processing according to a request every time that a performance of an operation is requested by a LAN.

Susaki fails to disclose this feature because a user authenticates some of the requests that come in from the LAN, and Shitama fails to discuss how requests are processed if they come in from the LAN.

Susaki discloses a client server system where a terminal 1 and a server 2 are connected through a communication network 3 such as a LAN (Fig. 1 and col. 5, lines 8-12). Susaki is directed to controlling access to a particular service by a user connected via the LAN in order to avoid leakage of official secrets and falsification of information (col. 1, lines 31-37). In order to achieve this, Susaki at col. 9, line 38 - col. 10, line 16 discusses using a service approval request processor 206 that determines if approval is required based on a process control rule. Based on the process control rule, a determination is made whether approval is not required (col. 9, lines 58-67), or if approval is required (col. 10, lines 1-16). Because approval may be required, Susaki fails to automatically accept requests that come in from the LAN as called for by independent claims 1, 11 and 20.

Shitama fails to discuss how requests are processed if they come in from the LAN because Shitama is instead directed to authenticating requests that come in from the WAN. Page 5 of the Office Action states "all requests from the LAN are trusted" and "implicitly allows all local requests for local resources". Although Shitama does disclose a LAN, Shitama fails to explicitly provide such disclosure.

Furthermore, pages 12 and 13 of the Office Action asserts that "it does not hold that all of the levels of scrutiny must be used in a combination with Shitama" and that "requests from the LAN are always fulfilled"; therefore, in combination with Susaki, one skilled in the art would "place all LAN address as having a user authority level of "0" in the table of Fig. 5." Applicants disagree. It is not reasonably predictable to discard the security provided for

requests that come in from the LAN as discussed by Susaki and to only apply it to requests that come in from the WAN in the manner suggest on pages 12 and 13 of the Office Action.

Applicants assert that, given the detail provided by Susaki as to how requests from the LAN are processed and the lack of detail provided by Shitama, one skilled in the art combining the disclosures of Susaki and Shitama would logically treat requests from the LAN as disclosed by Susaki (that is, some requests that come in from the LAN would require user approval). In other words, one skilled in the art would not automatically accept an operation according to the request every time that it is determined that the request came in from the LAN as called for by claim 1, for example. Furthermore, if one skilled in the art were to combine Susaki and Shitama (which Applicants do not admit would have been obvious), one skilled in the art would instead add the security for requests that come in from the LAN as disclosed by Susaki to the security for requests that come in from the WAN as disclosed by Shitame. Such a combination fails to suggest all of the features of independent claims 1, 11 and 20.

REQUESTS FROM THE WAN

Claims 1 and 20 call for a controller that allows a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN; and claim 11 calls for the step of allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN.

As discussed above, Susaki only discloses a client server system where the terminal 1 and server 2 are connected through a communication network 3 such as a LAN (Fig. 1 and col. 5, lines 8-12). Susaki never discusses the WAN, and the citations provided in the Office Action, for example on page 2, fail to discuss the WAN.

Shitama limits access from the WAN to the LAN by using a gateway 30 that authenticates all requests from the WAN using a predetermined authentication code and method. Shitama fails to provide any discussion with regard to allowing any user intervention. Therefore, Shitama suffers the same problems identified in paragraph [0003] of Applicants' specification in that passwords may be artificially leaked to outsiders as well as being leaked by stealing packets from a network.

For similar reasons discussed above, Applicants assert that, given the detail provided by Shitama as to how requests from the WAN are processed and the lack of any detail by Susaki, if one skilled in the art were to combine Susaki with Shitama, which Applicants do not admit would have been obvious, then one skilled in the art would have used Shitama's authentication procedure for requests that come in from the WAN. It would not have been reasonably predictable to discard Shitama's procedure for requests from the WAN in order to use Susaki, which is directed to requests from the LAN. Again, if one skilled in the art were to combine Susaki and Shitame (which Applicants do not admit would have been obvious), one skilled in the art would instead add the security for requests that come in from the LAN as disclosed by Susaki to the security for requests that come in from the WAN as disclosed by Shitame.

In addition, even if one skilled in the art would have used Susaki's procedure with Shitama, the combination still fails to suggest allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN as called for by claim 1, for example. As discussed above, Susaki allows a user to authenticate some requests and Shitama uses the gateway to authenticate all requests.

* * * * *

In view of at least the above, the combination of Susaki and Shitama fails to disclose or suggest all of the features in the independent claims as well as the features in the dependent claims. It is respectfully requested that the rejection be withdrawn.

Claims 2 and 12 were rejected under 35 U.S.C. §103(a) over Susaki in view of Shitama and Joubert et al. (Joubert), U.S. Patent No. 6,101,616, claims 5 and 14 were rejected under 35 U.S.C. §103(a) over Susaki in view of Shitama and Allen et al. (Allen), U.S. Publication No. 2003/0041333, and claims 10 and 19 were rejected under 35 U.S.C. §103(a) over Susaki in view of Shitama and Boehmke et al. (Boehmke), U.S. Publication No. 2002/0126822. The rejections are respectfully traversed.

None of Joubert, Allen and Boehmke overcome the deficiencies of Susaki and Shitama as applied to independent claims 1, 11 and 20. It is respectfully requested that the rejections be withdrawn.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Scott M. Schulte
Registration No. 44,325

JAO:SMS

Date: December 2, 2008

OLIFF & BERRIDGE, PLC
P.O. Box 320850
Alexandria, Virginia 22320-4850
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

UNITED STATES PATENT AND TRADEMARK OFFICE

FEB 27 2009

SMS

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/671,686	09/29/2003	Kazuma Aoki	117025	1077

25944 7590 12/23/2008

OLIFF & BERRIDGE, PLC
P.O. BOX 320850
ALEXANDRIA, VA 22320-4850

RECEIVED
DEC 24 2008

EXAMINER	
KEEFER, MICHAEL E	
ART UNIT	PAPER NUMBER
2454	

MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No.	Applicant(s)	
	10/671,686	AOKI ET AL.	
	Examiner	Art Unit	
	MICHAEL E. KEEFER	2454	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 02 December 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: 1-20.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Dustin Nguyen/
Primary Examiner, Art Unit 2454

Continuation of 11. does NOT place the application in condition for allowance because: Applicant argues that the combination of Susaki and Shitama does not teach all the limitations of claims 1 and 11. Specifically, Applicant alleges that the combination does not teach "determining between requests from the LAN and WAN" and performing exactly the same action every time a request is received from the LAN or WAN (i.e. allowing/asking for permission). First, the Examiner points to paragraphs 52-53, which disclose determining that a request came from a WAN (as opposed to the LAN) by determining what interface the request arrived from (Fig. 2, interfaces 33 and 34). One of ordinary skill in the art would be motivated to replace the security system provided by Shitama in gateway 30 with the security system provided by Susaki in order to allow the access to a service to be properly controlled (Susaki, Col. 2, lines 46-52). One of ordinary skill in the art would realize that from the teachings of Shitama, that is advantageous to screen requests coming in from the WAN, and that this can be accomplished without adding the additional overhead of encryption by using the approval system taught by Susaki. Further, since no scrutiny is applied to requests from the LAN in Shitama, one of ordinary skill in the art would be motivated to continue to trust all requests from the LAN .

US006189032B1

(12) **United States Patent**
Susaki et al.

(10) **Patent No.: US 6,189,032 B1**
(45) **Date of Patent: Feb. 13, 2001**

(54) **CLIENT-SERVER SYSTEM FOR CONTROLLING ACCESS RIGHTS TO CERTAIN SERVICES BY A USER OF A CLIENT TERMINAL**

(75) Inventors: **Seiichi Susaki**; **Hisashi Umeki**, both of Yokohama; **Katsuyuki Umezawa**, Kawasaki; **Seiji Miyazaki**; **Kazuo Matsunaga**, both of Yokohama; **Makoto Kitagawa**, Fujisawa, all of (JP)

(73) Assignee: **Hitachi, Ltd.**, Tokyo (JP)

(*) Notice: Under 35 U.S.C. 154(b), the term of this patent shall be extended for 0 days.

(21) Appl. No.: **09/015,220**

(22) Filed: **Jan. 29, 1998**

(30) **Foreign Application Priority Data**

Feb. 27, 1997 (JP) 9-043738

(51) **Int. Cl.**[7] **G06F 15/173**; G06F 15/16

(52) **U.S. Cl.** **709/225**; 709/203; 713/201

(58) **Field of Search** 709/216, 217, 709/218, 219, 203, 225, 223; 395/187.01, 188.01; 713/200, 201, 202

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,757,533	*	7/1988	Allen et al.	380/25
5,319,542	*	6/1994	King, Jr. et al.	705/27
5,361,359	*	11/1994	Tajalli et al.	713/200
5,483,658	*	1/1996	Grube et al.	713/200
5,572,673	*	11/1996	Shurts	713/200
5,729,734	*	3/1998	Parker et al.	707/9
5,748,896	*	5/1998	Daly et al.	709/223
5,815,574	*	9/1998	Fortinsky	380/25
5,835,726	*	11/1998	Shwed et al.	709/229
5,845,068	*	12/1998	Winiger	713/200
5,848,233	*	12/1998	Radia et al.	713/201
5,872,915	*	2/1999	Dykes et al.	395/188.01
5,893,128	*	4/1999	Nauckhoff	707/511
5,898,830	*	4/1999	Wesinger et al.	713/201
5,944,821	*	8/1999	Angelo	713/200
5,987,611	*	11/1999	Freund	713/201

OTHER PUBLICATIONS

Adam et al., "Security–Control Methods for Statistical Databases: A comparative Study", ACM Computer Surveys, pp. 515–556, Dec. 1989.*

Shackelford et al., "The Architecture and Implemtation of a Distributed Hypermedia Storage System", Hypertext '93 Proceedings, pp. 1–13, Nov. 1993.*

D.E.R. Denning, Cryptography and Data Security, published by Addison–Wesley Publishing Company, Inc.

* cited by examiner

Primary Examiner—Zarni Maung
Assistant Examiner—Jason D. Cardone
(74) *Attorney, Agent, or Firm*—Mattingly, Stanger & Malur, P.C.

(57) **ABSTRACT**

A client-server system is provided in which access to a service by a user can properly be controlled, even if an approval by another user is required for receiving the service. First, the server **2** executes a log-in processing by using a user identifier and password transmitted from the client terminal **2**, and a user control file **202**. Next, the server **2** executes a service control by using a service supply request transmitted from the client terminal **1** and a service control file **42** provided with the server. When the server determines that an approval by another user is required for providing the service, the server executes the approval request to the client terminal **1** that the concerned user uses. When the reply to the approval request is affirmative, the server executes the processing in accordance with the foregoing service supply request. When the reply is negative, the server informs to the user who made the foregoing service supply request that the approval is rejected.

17 Claims, 14 Drawing Sheets

42

SERVICE IDENTIFIER	USER AUTHORITY LEVEL	PROCESS CONTROL RULE
A	0	ALWAYS PROCESSIBLE
	1	APPROVAL BY "TARO" (IS) REQUIRED
	2	IMPOSSIBLE TO PROCESS
	3	IMPOSSIBLE TO PROCESS
	⋮	⋮
B	0	ALWAYS PROCESSIBLE
	1	ALWAYS PROCESSIBLE
	2	ALWAYS PROCESSIBLE
	3	ALWAYS PROCESSIBLE
	⋮	⋮
C	0	ALWAYS PROCESSIBLE
	1	APPROVAL BY ONE PERSON OF LEVEL 0 (IS) REQUIRED
	2	APPROVAL BY TWO PERSONS OF LEVEL 0 (IS) REQUIRED
	3	
	⋮	⋮
⋮	⋮	⋮

US 20020110123A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0110123 A1

Shitama (43) Pub. Date: Aug. 15, 2002

(54) NETWORK CONNECTION CONTROL APPARATUS AND METHOD

(76) Inventor: Kazuhiro Shitama, Chiba (JP)

Correspondence Address:
SONNENSCHEIN NATH & ROSENTHAL
P.O. BOX 061080
WACKER DRIVE STATION
CHICAGO, IL 60606-1080 (US)

(21) Appl. No.: 10/045,320

(22) Filed: Nov. 9, 2001

(30) Foreign Application Priority Data

Nov. 10, 2000 (JP) P2000-343429

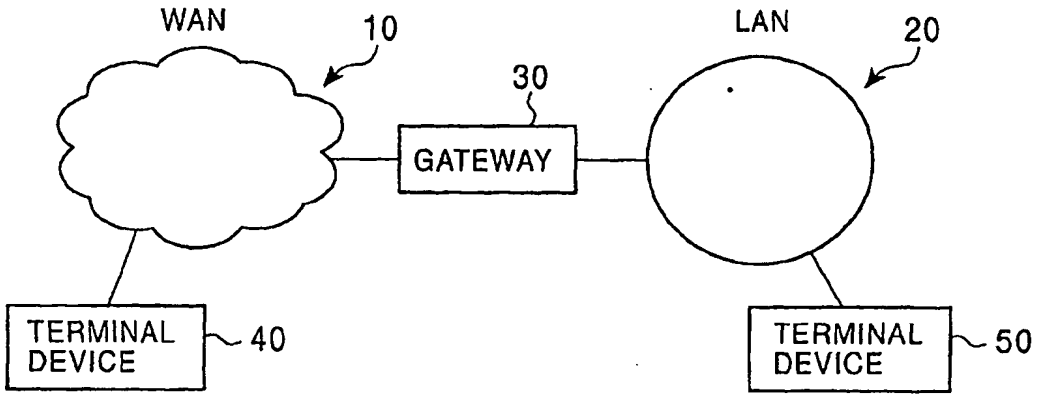
Publication Classification

(51) Int. Cl.[7] H04L 12/28

(52) U.S. Cl. 370/389; 370/401

(57) ABSTRACT

A network connection control apparatus and method are provided for granting access to an authenticated device on a global network to a device on a local network, wherein the access permission setting can be automatically controlled. The network connection control apparatus comprises an access control unit which authenticates the device on the global network which transmitted an access request, creates an access permission entry for the authenticated device, and adds the entry to an access permission list. Upon receiving a data packet from the device on the global network, the access control unit determines whether the data packet should be transferred to the local network on the basis of access information extracted from the data packet and the information about the access permission entry contained in the access permission list.



US006101616A

United States Patent [19]

Joubert et al.

[11] Patent Number: 6,101,616

[45] Date of Patent: Aug. 8, 2000

[54] DATA PROCESSING MACHINE NETWORK ARCHITECTURE

[75] Inventors: **Philippe Joubert**, Cesson-Sévigné; **Thierry Leconte**, Betton; **Bruno Rochat**, Pacé, all of France

[73] Assignee: **Bull S.A.**, Louveciennes, France

[21] Appl. No.: **08/887,254**

[22] Filed: **Jul. 2, 1997**

[30] **Foreign Application Priority Data**

Mar. 27, 1997 [FR] France 97 03778

[51] **Int. Cl.**[7] **G06F 11/16**; G06F 15/16

[52] **U.S. Cl.** **714/11**; 709/105

[58] **Field of Search** 714/4, 10, 11, 714/102, 104, 105; 709/6, 201, 205, 217–221, 226

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,891,810	1/1990	de Corlieu et al.	714/11
5,155,729	10/1992	Rysko et al.	714/11
5,423,024	6/1995	Cheung	714/11
5,774,660	6/1998	Brendel et al.	709/6 X
5,867,706	2/1999	Martin et al.	709/6

FOREIGN PATENT DOCUMENTS

0865180	9/1998	European Pat. Off. .
WO 9618149	6/1996	WIPO .

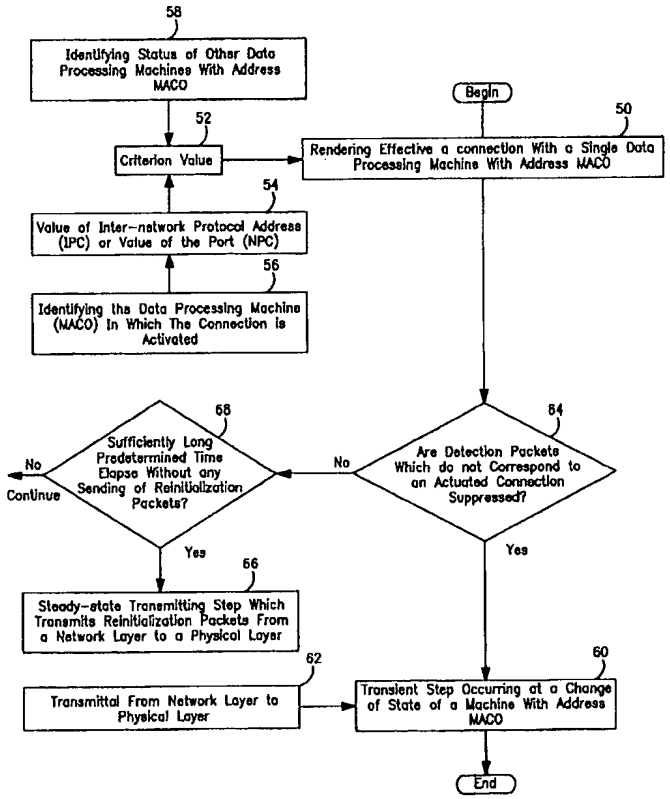
Primary Examiner—Thomas M. Heckler

Attorney, Agent, or Firm—Miles & Stockbridge P.C.; Edward J. Kondracki

[57] **ABSTRACT**

The invention relates to data processing machine network architecture and more particularly relates to the load balancing of data servers. A data server (3) is constituted by at least two server data processing machines (1, 2) capable of providing the same services. The server data processing machines (1, 2) have the same physical address MAC0 to which the same network protocol address is assigned in order to establish connections of client machines to the server (3), which is considered as a single virtual machine. Each server data processing machine comprises filtering means so that each connection of a client machine (5, 6, 7, 8, 9, 10) to the virtual machine corresponds to a unique connection effective with one and only one server data processing machine (1 or 2). The filtering means of each server data processing machine (1, 2) take into account at least one indicator of the status of each server data processing machine (1, 2) having the same physical address MAC0.

7 Claims, 6 Drawing Sheets



US 20030041333A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0041333 A1

Allen et al. (43) Pub. Date: Feb. 27, 2003

(54) SYSTEM AND METHOD FOR AUTOMATICALLY ANSWERING AND RECORDING VIDEO CALLS

(76) Inventors: Paul G. Allen, Mercer Island, WA (US); Michael E. Sears, Bellevue, WA (US); John M. Kellum, Seattle, WA (US)

Correspondence Address:
DIGEO, INC C/O STOEL RIVES LLP
201 SOUTH MAIN STREET, SUITE 1100
ONE UTAH CENTER
SALT LAKE CITY, UT 84111 (US)

(21) Appl. No.: 09/940,181

(22) Filed: Aug. 27, 2001

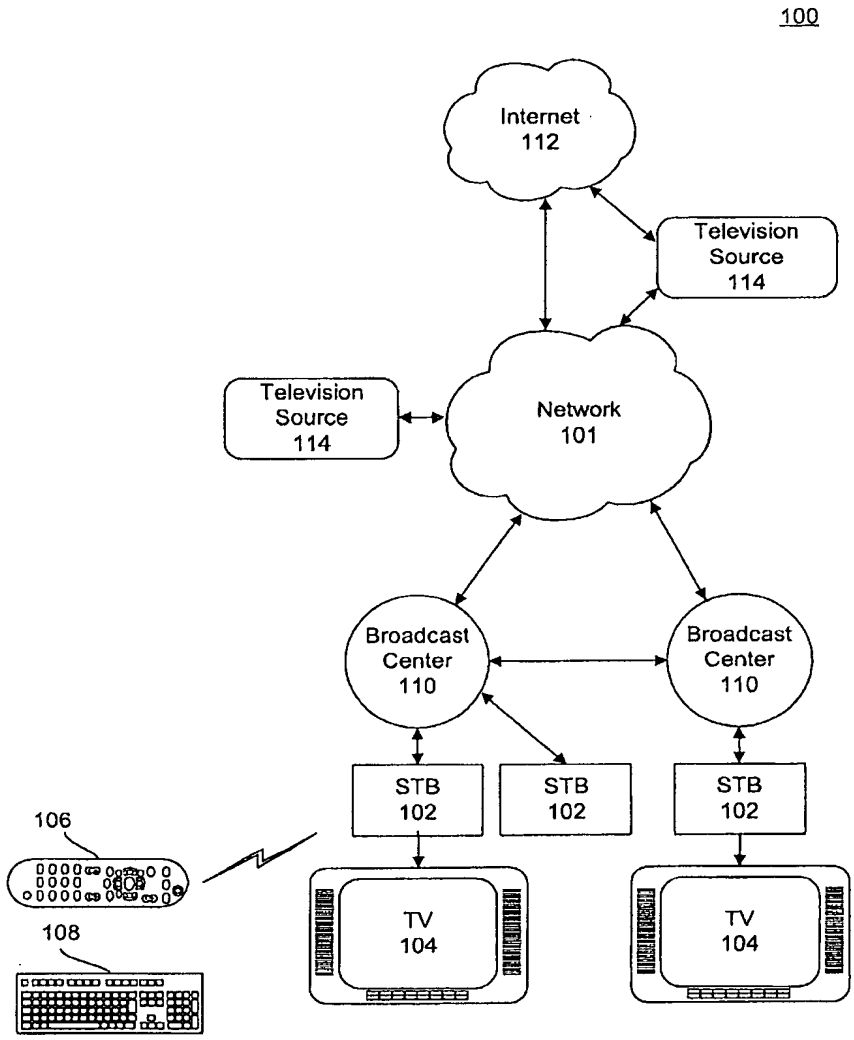
Publication Classification

(51) Int. Cl.[7] H04N 7/173

(52) U.S. Cl. 725/106; 725/122

(57) ABSTRACT

A request to establish video communication between a caller and a user of an interactive television system is detected. The caller is identified using information contained within the request. The user is prompted to accept or reject the request. In response to the user rejecting the request or not accepting the request within an established time interval, a pre-recorded video greeting is sent to the caller. Thereafter, a video message is recorded including a video signal received from the caller. While the video message is being recorded, the user may interrupt the recording to establish two-way video communication with the caller.



US 20020126822A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0126822 A1

Boehmke et al. (43) Pub. Date: Sep. 12, 2002

(54) SYSTEM, METHOD AND APPARATUS FOR CAPTURING AND PROCESSING CALL PROCESSING FAILURES OCCURRING AT A TELEPHONE SWITCH CONTROL PROCESSOR

(76) Inventors: **Yuergen Boehmke**, Parkland, FL (US); **Kenneth L. Shepard**, Boca Raton, FL (US)

Correspondence Address:
Roberto Capriotti, Agent
Kirkpatrick & Lockhart LLP
Henry W. Oliver Bldg.
535 Smithfield Street
Pittsburgh, PA 15222-2312 (US)

(21) Appl. No.: **09/746,505**

(22) Filed: **Dec. 22, 2000**

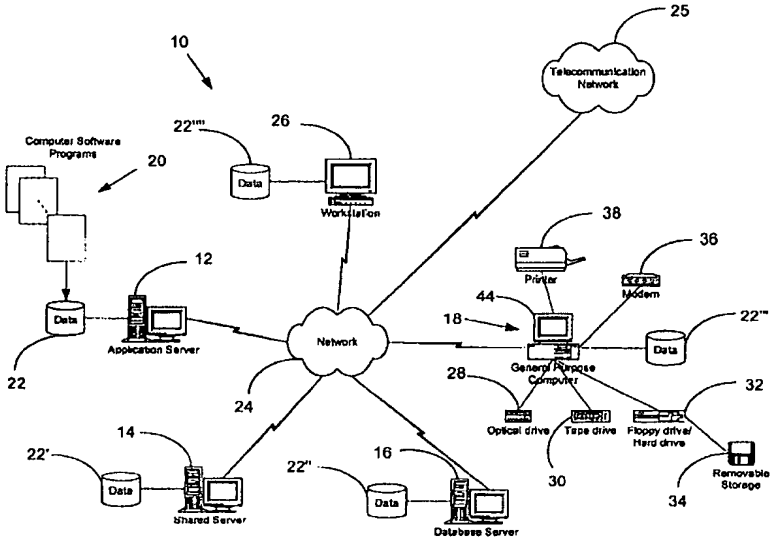
Publication Classification

(51) **Int. Cl.**[7] **H04M 7/00**; H04M 3/00

(52) **U.S. Cl.** **379/221.03**; 379/279

(57) ABSTRACT

A system, method and apparatus is disclosed for capturing call processing failures in a telecommunication system occurring at a telecommunication switch control processor as the failures occur. The system includes a computing system adapted for communicating with the telecommunication system. The computing system includes one or more computers having one or more processors for executing logic instructions; a memory associated with the computing system for storing the instructions; a storage device adapted for communicating with the computing system for storing data; and a communication device associated with the computing system for establishing a communication link between the computing system and the telecommunication system. The logic instructions are executed by the computing system and cause the one or more processors to establish a communication link between the computing system and the telecommunication system; continually capture call processing failure data occurring at the telecommunication switch control processor; and store the captured call processing failure data to the storage device. The method includes establishing a communication link between a computing system and the telecommunication system; the computing system continually capturing call processing failure data occurring at the telecommunication switch control processor; and storing the captured call processing failure data to the storage device. The apparatus includes a computer adapted for communicating with the telecommunication system, the computer having one or more processors to execute logic instructions associated with one or more computer software programs and a memory for storing the logic instructions; a first adapter coupled to the computer for interfacing the computer to a server; a second adapter coupled to the computer for continually capturing call processing failure data at the telecommunication switch control processor; and a communication device coupled to the computer for establishing a communication link between the computer and the telecommunication system.



XV. APPENDIX E - RELATED CASES APPENDIX

NONE